NOTICE: When government or other drawings, specifications or other data are used for any purpose other than in connection with a definitely related government procurement operation, the U. S. Government thereby incurs no responsibility, nor any obligation whatsoever; and the fact that the Government may have formulated, furnished, or in any way supplied the said drawings, specifications, or other data is not to be regarded by implication or otherwise as in any manner licensing the holder or any other person or corporation, or conveying any rights or permission to manufacture, use or sell any patented invention that may in any way be related thereto.

NRL Report 5730

SOME ASPECTS OF GO/NO-GO TESTING OF RANDOMNESS OF CONTINUALLY GENERATED BINARY DIGITS

H. M. Suski

Security Systems and Avigation Branch
Electronics Division

March 1, 1962

U. S. NAVAL RESEARCH LABORATORY
Washington, D.C.

CONTENTS

ABSTRACT

Pseudorandom numbers can be obtained statically, i.e., from a table of random numbers, or they may be generated continually (dynamically). Static cases have been investigated; e.g., tables of random digits often contain results of tests. The dynamic case, however, implies that tests for randomness be made continually. Go/no-go methods are attractive.

Problems associated with measuring randomness in the dynamic case of a generator continually producing binary digits are investigated. The mathematics of Bernoulli trials serves as the model against which the performance of the generator is compared. It is shown that there are a large number of ways in which a measuring system might be attempted. Such systems are based on explicit functions (called measure functions) of p, the probability that a "one" is generated.

Since the digits can be grouped (a group consists of m digits), a binomial expansion $[p + (1 - p)]^m$ can be written for each value of m. Any term or combination of terms of any expansion can serve as a measure group, the basis of a measure function.

A typical measuring problem involves the case where p is constant and has a value within specified tolerances. A go/no-go measurement indicates that p is within the specified tolerances. Means are provided for the setting of measure group-count t, .erances; a count alone then provides the indication of an acceptable or nonacceptable value of p. The sample size is selected on the basis of the desired confidence limit or the upper bound of the error in measuring p.

Since there are many possible measure functions, some means is required for comparing the relative effectiveness of different functions. A useful method of comparison is available if measure function "acceptance" characteristics are plotted. An acceptance characteristic is a plot of the probability that the measure group digits occur within the determined group-count tolerances. The acceptance characteristic is plotted for the results obtained from a single application of a particular measure function. By requiring a sequence of applications of the same measure function and by introducing an acceptance decision criterion, the acceptance characteristic more nearly approaches the ideal.

ABSTRACT (Continued)

Under certain conditions, a failure of the generator might manifest itself by the appearance of a repeated sequence of digits. Some of the necessary conditions are investigated for a go/no-go measuring system to breakdown, i.e., to give erroneous "accept" or "go" readings for an input consisting of specific repeated sequences. It is found that immunity from breakdown is dependent upon the number of digits in the group used in the measure function; the longer the group, the longer is the sequence of digits which can cause an erroneous indication – thus, more immunity.

The various aspects of the problem of a dynamic measurement of randomness are illustrated in an arbitrary example. Results are obtained for three measure functions.

In developing the theory, a method for measuring p was obtained; it provided an independent method useful in checking the go/no-go results.

PROBLEM STATUS

This is an interim report on a phase of the problem; work is continuing on this and other phases of the problem.

AUTHORIZATION

NRL Problem R03-01
Projects RF 001-10-41-4150, SF 001-10-01-6106, 6108,
and RAV 52 R002/652-1/F001-10-001

Manuscript submitted November 9, 1961.

SOME ASPECTS OF GO/NO-GO TESTING OF RANDOMNESS OF CONTINUALLY GENERATED BINARY DIGITS

INTRODUCTION

There are two ways in which random or, more appropriately, pseudorandom numbers can be obtained. The numbers can be taken from a table, i.e., statically, or, they can be created continually (dynamically) and used as required. In the past, a number of (static) tabulations satisfied the needs. With the increased use of high-speed computers, the need for generating pseudorandom digits continually (dynamically) has also increased. Routines are available which can be used by specific computers to create pseudorandom digits as the machine requires them. There are other means for creating digits randomly.*

Regardless of how the digits are generated, the problem remains to determine if the digits produced are random. In the static case of a tabulated set of digits, the tabulation is subjected to a set of statistical tests.* The fact that the table was published indicates that the conclusion drawn from the tests is that the entries are random with a high enough degree of confidence. In the dynamic case, where the random digits are produced continually, repeated testing is necessary if the process of generating digits is to be checked. In the case of a computer routine, the routine is selected because the digits produced will exhibit random properties. The problem of testing the randomness of digits produced continually does not appear to have been explored. It is this problem which is being investigated in this report.

We will concern ourselves more specifically with the problem of investigating the measurement of randomness of continually generated, random, binary digits. As it turns out, there are a large number of ways of making the measurement, and each method can be adapted for testing any set of random numbers. While the static case permits a more leisurely approach to the measurement of randomness, the dynamic case presents the unique situation of continually requiring rapid evaluations of the numbers being generated. Because of its attractiveness for the indicated purpose, a go/no-go method of measurement is being investigated. Since go/no-go methods suggest unattended operation, a detailed examination is appropriate to establish the likely limitations which are an inherent part of the method.

It will be shown that the measuring method depends upon the probability p that the digit generated is a "one." There are a variety of relationships, explicit functions of p, which can be formed; relations called measure functions are derived. The manner in which measure functions can be obtained and applied is indicated. To illustrate the application of the measuring technique, three measure functions are treated in an arbitrary problem (arbitrary because any specific problem requires a prior statement of the tolerances in the value of p which will be permitted). In the illustrative example, three measure functions are compared, and it is concluded that effective results are obtainable.

As a subsidiary result, a means is obtained for the measurement of p. This result provides an independent method which can be used in checking results obtained by go/no-go methods.

*See the introductory remarks on the production of random digits and the tests for randomness in the Rand Corporation's "A Million Random Digits, with 100,000 Normal Deviates," The Free Press, 1955.

THEORY

Introduction

Let us examine a process whose output is a sequence of binary digits. Suppose we arrange the sequence, as it is created, into groups of m digits each. If we list the m-digit groups in order, as they are generated, we can form for n such groups an array of digits as follows:

$$\begin{matrix} b_{11} & b_{12} & \cdot\ \cdot\ \cdot & b_{1m} \\ b_{21} & b_{22} & \cdot\ \cdot\ \cdot & b_{2m} \\ \vdots & \vdots & & \vdots \\ b_{i1} & b_{i2} & \cdot\ \cdot\ \cdot & b_{im} \\ \vdots & \vdots & & \vdots \\ b_{n1} & b_{n2} & \cdot\ \cdot\ \cdot & b_{nm} \end{matrix} \tag{1}$$

where

$$b_{im} = 0 \text{ or } 1, \qquad (i, j = 1, 2, \ldots) \tag{2}$$

since we are dealing with binary numbers. The n by m array has n rows and m columns. Consider any arbitrary column, say the mth. We can say that

$$\sum_{i=1}^{n} b_{im} = n_m(1) \tag{3}$$

where n_m is the number of ones in the column. If we let n increase without limit, then we can define

$$\lim_{n \to \infty} \frac{1}{n} \sum_{i=1}^{n} b_{im} = p_m \tag{4}$$

as the probability of a one occurring anywhere in the column. Thus, if the process is statistically stable, or n is large enough,

$$\frac{n_m(1)}{n} \sim p_m . \tag{5}$$

Since

$$n_m(1) + n_m(0) = n \tag{6}$$

then

$$n_m(0) = n - n_m(1) \tag{7}$$

or, in terms of p_m and q_m,

$$q_m = 1 - p_m, \text{ i.e., } p_m + q_m = 1 \tag{8}$$

where q_m is the probability of a zero occurring anywhere in the column. In the same way, values of p_m and q_m can be obtained for any m. In fact, a value of p can be obtained by extracting a sample of any μ digits from the array given in (1). In such a case, the number of ones in the sample is defined as $\mu(1)$, and

$$\frac{\mu(1)}{\mu} \sim p, \ 0 < \mu \leq n_m. \qquad (9)$$

We can see that (9) gives the general form of a system of measurement of p. However, it involves the counting of digits, or summing operations, and the operation of division. It is desirable to use, if possible, only the summing of digits in a system of measurement.

Upon examination of (1) we find that for a finite value of n and for a given array we can form a number of groupings, each of which contain μ digits, and that this number of groupings is the number of combinations of nm things taken μ at a time $\binom{nm}{\mu}$. Hence, if we take a large enough number of groupings, we obtain a sequence of numbers

$$\mu_1(1), \ \mu_2(1), \ \mu_3(1), \ldots \qquad (10)$$

and if these numbers are "statistically consistent," we might conclude that there is a single value of p which can describe the digit generating process. In other words, we conclude that the array of digits was produced under the condition that p, the probability of a one occurring anywhere in the array is constant. We are drawn to the conclusion that, ideally, the digit generating process is exactly that of Bernoulli trials. Consequently, we look to the binomial distribution to guide us to the meaning of the term "statistically consistent" as used with (10). The binomial distribution is given by *

$$B(\mu, k, p) = \binom{\mu}{k} p^k q^{\mu - k}, \qquad (k = 0, 1, 2, \ldots, n) \qquad (11)$$

where $B(\mu,k,p)$ is the probability that in a sample of size μ, exactly k ones will be present; i.e., $k = \mu(1)$. Using (11) we can calculate the variation in k to be expected in the ideal case. A basic aspect of the method of measuring randomness lies in the comparison of the performance of an actual process with that of the ideal process of Bernoulli trials.

Measure Groups

In (11) the function involves p directly; it is a simple function. The use of (11) as just indicated seems to imply the test of static situations, i.e., tests using a single array as indicated in (10). In a dynamic case, different arrays would be involved. In a dynamic case, either a single test or a number of tests such as (10) might be performed; the implicit assumption is made that p remains constant (or, equivalently, that p remains within tolerable limits) for each array tested.

Returning for another look at (1) we note that the generated sequence of digits is arranged in groupings of m digits each. In the above discussion we approached the array essentially through the columns. Now, suppose we consider the rows. With m digits in each row, we can form 2^m arrangements of the m binary digits. From entries in an array we can form digits, in essentially a new number system, in whatever fashion we desire. If we care to do so for any particular array, we find that we can form $\binom{nm}{n}$ combinations of nm things taken m at a time. If we wish to examine a sample size of μ digits in the transformed number system, we would find that we could form $\binom{\binom{nm}{m}}{\mu}$ samples. In this case, as in the previous case, a static analysis can be made, or the analysis can be made dynamically.

*See W. Feller, "An Introduction to Probability Theory and its Applications," Vol. I, p. 106, New York:Wiley, 1950.

It is clear that no restriction has been placed on the value of m. This discussion indicates that we may exhaustively test arrays, either statically or dynamically. We will not consider any further here the extent to which we must go toward exhaustiveness. Instead, we will consider what can be expected from making single tests, or a small number of tests.

We have thus far indicated a simple function involving p itself. We also indicated that we might treat groupings of the digits by effectively treating the digits of a number system with a higher order base, or radix, 2^m. The simple function consists of considering single digits. We could just as well consider 2, 3, 4, or more digits together, and examine their occurrences. This is equivalent to taking m = 2, 3, 4, etc. By the same process which led to (8), we can obtain the relations for the probability of occurrence of specific pairs, triples, quadruples, or quintuples of digits from the following relations:

$$\begin{aligned}
&q + p = 1, && (m = 1)\\
&q^2 + 2pq + p^2 = 1, && (m = 2)\\
&q^3 + 3pq^2 + 3p^2q + p^3 = 1, && (m = 3)\\
&q^4 + 4pq^3 + 6p^2q^2 + 4p^3q + p^4 = 1, && (m = 4)\\
&q^5 + 5pq^4 + 10p^2q^3 + 10p^3q^2 + 5p^4q + p^5 = 1, && (m = 5)
\end{aligned} \tag{12}$$

and so on. These terms are obtained from the binomial expansion of $(q + p)^m$.

At this point, let us consider a specific, but arbitrary, choice of a new radix. Suppose we take $m = 4$. Then $2^m = 2^4$, and we have a radix of 16, or what is often referred to as the hexadecimal number system. While we will use this radix value throughout the remainder of this report, other values could be used as well. For this case, the binary combinations of the four digits are shown in Fig. 1(b), together with commonly used hexadecimal digital equivalents and expressions for the probabilities of occurrences of each of the hexadecimal digits. Several possibilities are available to us. We can use any one of the hexadecimal digits as an indirect measure of p, or we can use various groupings of these digits. Among the possible groupings of digits, we can treat together those digits which contain various numbers of ones. In this way we can form five groups, those varying in content from none to four ones. Forming the individual probabilities (Fig. 1(b)), for these groups of digits and taking their sum, i.e., the probability that any of the groups will occur, we write

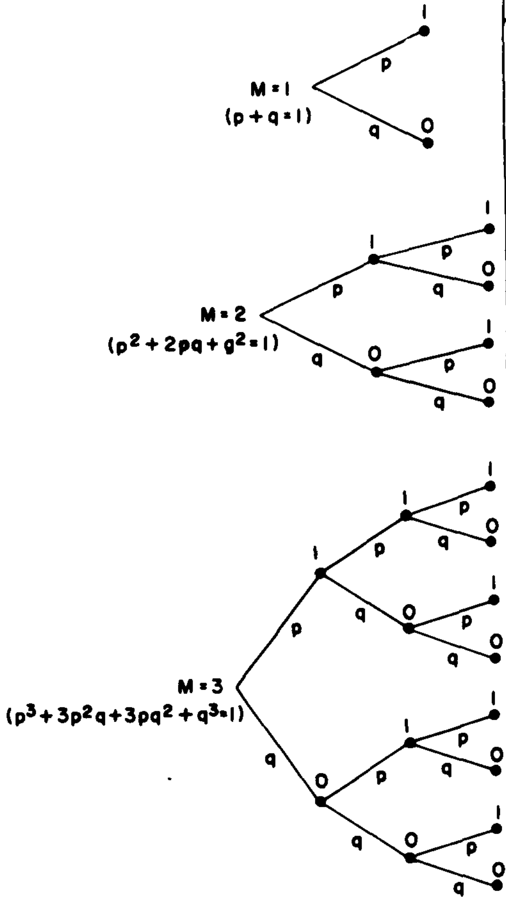
$$q^4 + 4pq^3 + 6p^2q^2 + 4p^3q + p^4 = 1. \tag{13}$$

We can, furthermore, combine terms of (13) as follows:

$$(q^4 + 4pq^3) + (6p^2q^2) + (4p^3q + p^4) = 1. \tag{14}$$

We see that there are a variety of ways of forming groups of hexadecimal digits. Any one of the groupings in (13) or (14) forms a valid function which can be used in the indirect measurement of p. In a similar way, we can form groups of digits with any of the terms or combinations of terms given in (12). The actual groupings which can be obtained are shown in Fig. 1. It is possible to form other groupings by taking higher values of m.

Since there are a number of choices to be made with regard to possible groupings, we will have to consider ways of comparing the results obtained by using a number of the functions; the functions we use will be called measure groups. We will consider three measure groups later as part of an illustrative example. Now we wish to see how we can adapt any of these functions to a scheme of measurement.



2^M NUMBER SYMBOLS	PROBABILITY OF OCCURRENCE OF DIGITAL GROUPS OR SYMBOLS
1	p
0	q
3	p^2
2	pq
1	pq
0	q^2
7	p^3
6	p^2q
5	p^2q
4	pq^2
3	p^2q
2	pq^2
1	pq^2
0	q^3

(a)

Fig. (1) - Schematic or tree of (a) one-, two-, and three-bit processes (m= 1,2,3), (b) a four-bit process (m = 4), and (c) a five-bit process (m = 5)

We have already indicated how, with (11) and the function $B(\mu,k,p)$, comparisons can be made with the ideal case or model – only the count of ones is required. The use of (11) applies as well to the case where compound functions, as in (13) or (14), are involved. Let us consider the first term of (13) as a measure group; it is a compound function of p because it is composed of four digits, which are all zeros. Let

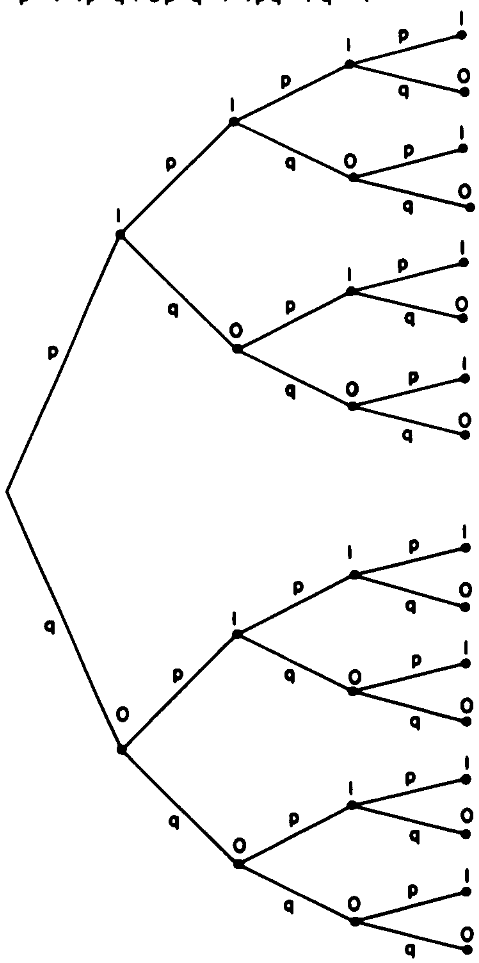
$$p_g = q^4 \tag{15}$$

be the probability that the binary group 0000, or the hexadecimal digit 0, has occurred. Then

$$q_g = 1 - q^4 = 1 - p_g . \tag{16}$$

M = 4

$p^4 + 4p^3q + 6p^2q^2 + 4pq^3 + q^4 = 1$



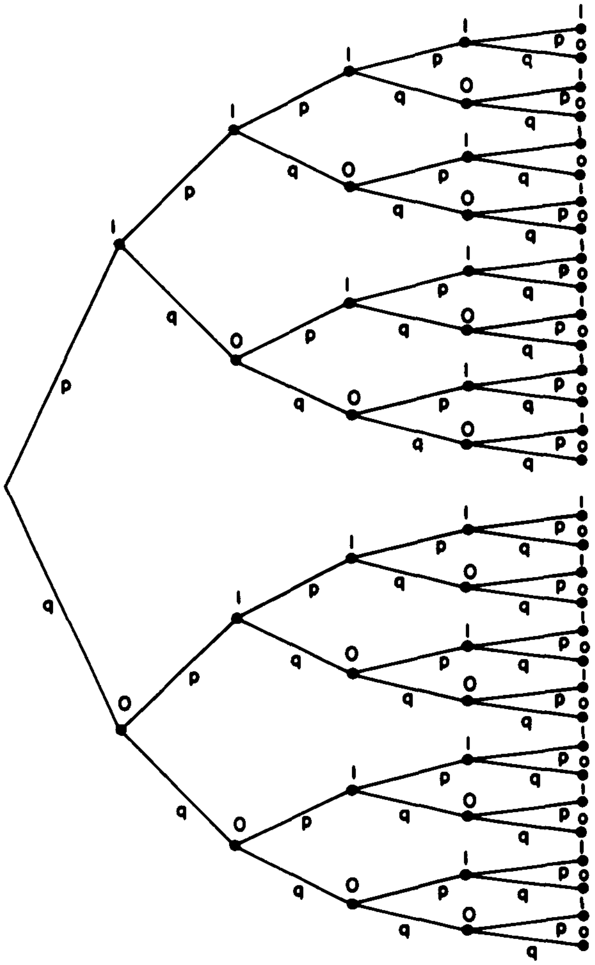
$2^{M=4}$ HEXA-DECIMAL NOTATION	PROBABILITY OF OCCURRENCE OF DIGITAL GROUPS OR SYMBOLS
f	p^4
e	p^3q
d	p^3q
c	p^2q^2
b	p^3q
a	p^2q^2
9	p^2q^2
8	pq^3
7	p^3q
6	p^2q^2
5	p^2q^2
4	pq^3
3	p^2q^2
2	pq^3
1	pq^3
0	q^4

(b)

Fig. 1 (Continued) - Schematic or tree of (a) one-, two-, and three-bit processes (m = 1,2,3), (b) a four-bit process (m = 4), and (c) a five-bit process (m = 5)

M = 5

$p^5+5p^4q+10p^3q^2+10p^2q^3+5pq^4+q^5 = 1$



$2^{M=5}$ NUMBER SYMBOLS	PROBABILITY OF OCCURRENCE OF DIGITAL GROUPS OR SYMBOLS
v	p^5
u	p^4q
t	p^4q
s	p^3q^2
r	p^4q
q	p^3q^2
p	p^3q^2
o	p^3q^2
n	p^4q
m	p^3q^2
l	p^3q^2
k	p^2q^3
j	p^3q^2
i	p^2q^3
h	p^2q^3
g	pq^4
f	p^4q
e	p^3q^2
d	p^3q^2
c	p^2q^3
b	p^3q^2
a	p^2q^3
9	p^2q^3
8	pq^4
7	p^3q^2
6	p^2q^3
5	p^2q^3
4	pq^4
3	p^2q^3
2	pq^4
1	pq^4
0	q^5

(c)

Fig. 1 (Continued) - Schematic or tree of (a) one-, two-, and three-bit processes (m = 1,2,3), (b) a four-bit process (m = 4), and (c) a five-bit process (m = 5)

From (13) and (16)

$$q_g = (4pq^3 + 6p^2q^2 + 4p^3q + p^4) \tag{17}$$

or, the probability that the measure group has not occurred is just the probability that any one of the other groups has occurred. This leaves us with a binary situation, which can be treated using the binomial law. Thus, a measure group can be transformed into a new variable and its complement by (15) and (17). Note that in a dynamic situation both p_g and q_g will be constant as long as p is constant with respect to time.

We can rewrite (11) for the new variable and for a sample size of n as

$$B(n,k,p_g) = \binom{n}{k} p_g^k \, q_g^{n-k} \tag{18}$$

for which can be obtained the probability that there will be exactly k occurrences of the particular group out of a sample of n trials. We can think of k as being the reading of a counter which gives the equivalent value of $n(g)$, the number of expected occurrences of the special measure group chosen. Thus, k becomes a measure of p_g. However, we can only conclude from a given reading which falls within the range of expected values of k that the process is following the model or ideal case. We can visualize a particular test situation in which both n and k are fixed, and we do not know the value of p_g. We will find that there can be a range of values of p_g which could probably have given the specific counter reading. We seek a range of values of k which will permit us to conclude that p_g is within allowable tolerances. We are concerned in (18) with three variables: n, k, and p_g.

Upper Bound of Error in p

Since we made use of a limiting process in defining p in (4), it is appropriate to turn to the law of large numbers. We seek a relation between n, k, and p_g. The law of large numbers may be expressed* as follows:

$$\Pr\left\{\left|\frac{k}{n} - p_g\right| < \epsilon\right\} \approx \Phi\left[\epsilon\left(\frac{n}{p_g q_g}\right)^{1/2}\right] - \Phi\left[-\epsilon\left(\frac{n}{p_g q_g}\right)^{1/2}\right] \tag{19}$$

or

$$\Pr\left\{\left|\frac{k}{n} - p_g\right| < \epsilon\right\} \to 1, \tag{20}$$

that is, certainty as n increases. In these statements ϵ is a preassigned small number, selected suitably to the conditions of the problem, which represents the measuring error or difference to be expected between k/n and p_g. The right-hand side of (19) is the difference between two values obtained from tables† of the normal distribution function (or the normal cumulative distribution function). The terms of (19) are of the form

$$\Phi(x) = \int_{-\infty}^{x} \phi(t)\,dt \tag{21}$$

where

$$\phi(t) = \frac{1}{\sqrt{2\pi}} e^{-(t^2/2)} \tag{22}$$

is the normal density function.

*Feller, op. cit., p. 137.

†op cit. pp. 136 and 137.

The difference on the right-hand side of (19) is called the confidence limit and, as given, shows that equal areas of the distribution function are excluded at either end (i.e., extreme positive and negative values are excluded). For the case where a 95 percent confidence limit is desired, 95 percent of the area under the distribution function is taken into consideration. Furthermore, half the difference, or 2.5 percent of the area, is excluded at either end. Thus, when tables of $\Phi(x)$ are available,

$$\Phi\left[\epsilon\left(\frac{n}{p_g q_g}\right)^{1/2}\right] \geq 0.95 + 0.025 = 0.975 \qquad (23)$$

hence,

$$\epsilon\left(\frac{n}{p_g q_g}\right)^{1/2} \geq 1.96. \qquad (24)$$

Therefore, we can tabulate the following values of n and ϵ (both numeric) for assumed values of p_g with 95 percent confidence:

n	ϵ
100	0.1
1,000	0.03
10,000	0.01
100,000	0.003

The effect of choosing different confidence limits is shown in Fig. 2 for values of p_g between 0.3 and 0.7. The use of Fig. 2 permits one to make a graphical selection of n, once the error in measuring p_g has been selected. Using the uppermost line in Fig. 2 for selecting n provides a reasonable upper bound for the error.

Use of Fig. 2 permits the selection, in practice, of a suitable measuring error. The desired error, however, is that in p, rather than in p_g. The relation between the relative error in p_g and that of the relative error in p is derived in Appendix B. It is shown that Fig. 2 still serves a useful purpose in determining the magnitude of the likely measuring error to be encountered and still permits the selection of value of n.

Measure Function

Next, as a means for approximating the expected limits of k, use can be made of the De Moivre-Laplace limit theorem* which states the equivalence

$$B(n,k,p_g) \approx \frac{1}{\sqrt{2\pi n p_g q_g}} \exp - \left[\frac{(k-np_g)^2}{2np_g q_g}\right]. \qquad (25)$$

The equivalence given in (25) is subject to the condition that

$$\frac{(k-np_g)^3}{n^2} \to 0, \qquad \text{or} \qquad n\epsilon^3 \to 0. \qquad (26)$$

In (25) and (26), np_g is the average number of occurrences of the particular grouping, $(k-np_g)$ is a deviation from the average value, and $np_g q_g$ is the variance (σ^2).

*W. Feller, op. cit., pp. 133-137.

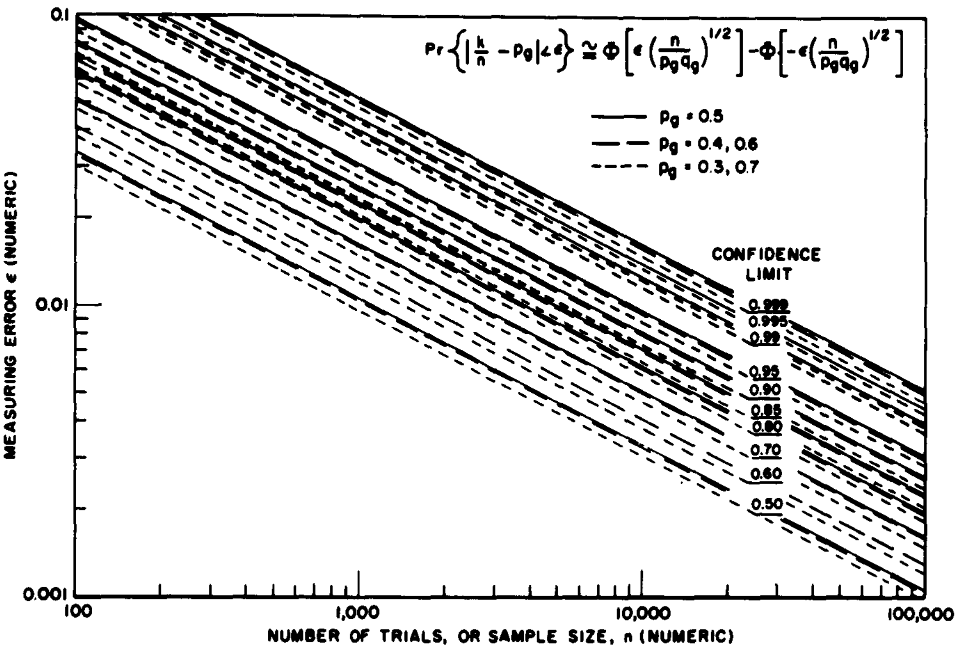


Fig. 2 - The measuring error as a function of the number of trials. For a choice of confidence limit, selecting ϵ will give n.

By making the substitutions

$$h = (np_g q_g)^{-1/2} \tag{27}$$

and

$$x_k = (k - np_g)h \tag{28}$$

we can rewrite (25) in the form of

$$B(n,k,p_g) = h\phi(x_k) \tag{29}$$

where

$$\phi(x_k) = \frac{1}{\sqrt{2\pi}} e^{-x_k^2/2} \tag{30}$$

is the normal density function. It can be shown* that (29) can be expressed with little error by

$$h\phi(x_k) \approx \int_{x_k-h/2}^{x_k+h/2} \phi(t)\, dt = \Phi\,(x_{k+1/2}) - \Phi\,(x_{k-1/2}). \tag{31}$$

The numerical evaluation of (18) is possible with the aid of (31) and tabulations of the normal distribution function. We have inaicated that we will be concerned about a range of values of k. Therefore, we are concerned about the function

$$M(k_1,k_2,n,p_g) = \sum_{k=k_1}^{k_2} \binom{n}{k} p_g^k\, q_g^{n-k} \tag{32}$$

*W. Feller, op. cit., p. 137.

which gives the probability that the reading will be in the interval $k_1 \leq k \leq k_2$, this function is called a measure function. It can be shown* that

$$M(k_1, k_2, n, p_g) = \Phi\,(x_{k_2+1/2}) - \Phi\,(x_{k_1-1/2}). \tag{33}$$

With the aid of tables of the normal probability function (if necessary, transformations given in Appendix A can be used), a good approximation of (32) is obtained. It is interesting to note that condition (19) is a special case of (33).

Validity Condition

In choosing specific values of x, care must be taken to keep within condition (26) on which the normal law approximation was based. Condition (26) may be restated as

$$x_k{}^3 h p_g{}^2 q_g{}^2 \longrightarrow 0. \tag{34}$$

Condition (34) establishes the validity of the application of the De Moivre-LaPlace limit theorem (25) and (33). Feller† demonstrates that (34) is satisfied, in many applications, for values of x_k of 3 or 4. With x_k between 3 and 4 and n between 10 and 100, the limit of acceptability can be written as

$$x_k{}^3 h p_g{}^2 q_g{}^2 \leq 1. \tag{35}$$

It follows that a maximum usable value of x_k is

$$x_k{}^3 \leq h^3 n^2 \qquad \text{or} \qquad x_k \leq h(n)^{2/3}. \tag{36}$$

Note that for larger values of , the left-hand side of (35) becomes much less than 1 with $x_k = 4$.

Count (k) Tolerances

Each term on the right-hand side of (33) is a normal distribution function, and (36) gives half the range for which reasonable approximations are valid. The fact that these terms are normal distribution functions can be used to some advantage when it is found necessary to go beyond the validity range given by (36). This fact will become evident as the discussion proceeds.

As a first approximation, the special value $x_k = 0$ can be used in setting tolerances, i.e., in finding values for k_1 and k_2. When $x_k = 0$, it follows from (28), and because $h \neq 0$, that

$$k = k_o = np_g. \tag{37}$$

Specifically, the assigned limits will be the lower limit

$$k_1 = np_{g_1} \tag{38a}$$

and the upper limit

$$k_2 = np_{g_2} \tag{38b}$$

*Feller, op. cit., p. 137.

†op. cit. pp. 136 and 137.

where p_{g_1} and p_{g_2} are either given directly or must be calculated from given values of p. In the latter case, the transformation between p and p_g can be performed graphically with the aid of Fig. 3, or an expanded version of p_g vs p for the specific measure group, similar to Fig. 4.

The fact that both terms of (33) are normal distribution functions permits, with the aid of probability graph paper, the use of graphical techniques in adjusting the tolerances. It is possible, also, to show graphically the expected range of variation in k about a selected tolerance. By solving (28) for k and using (27), we obtain

$$k = np_g \pm x_k \sigma = k_o \pm x_k \sigma . \qquad (39)$$

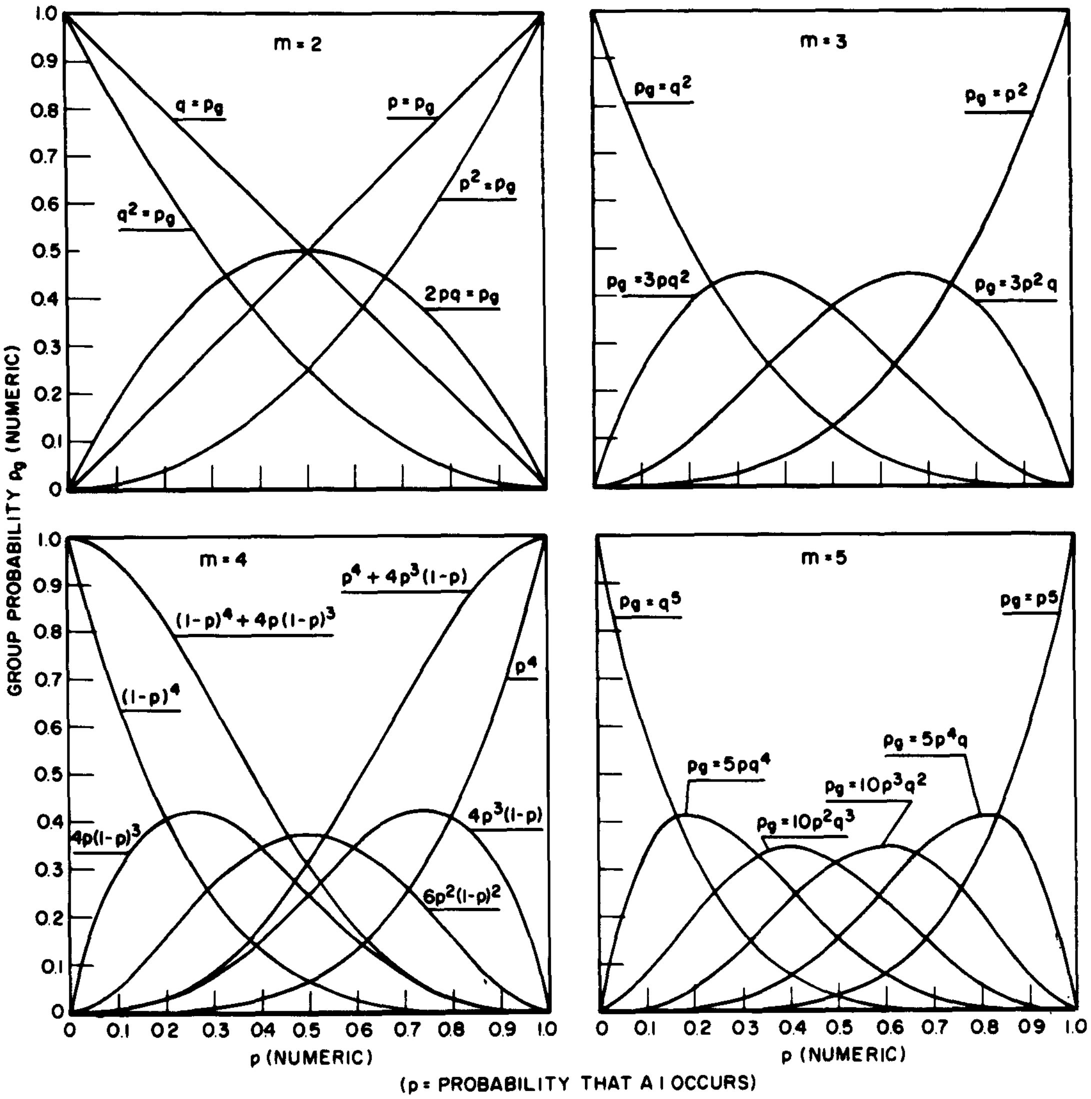


Fig. 3 - Graphical representation of transformations between p and p_g for the measure groups (values of m, or number symbols) indicated

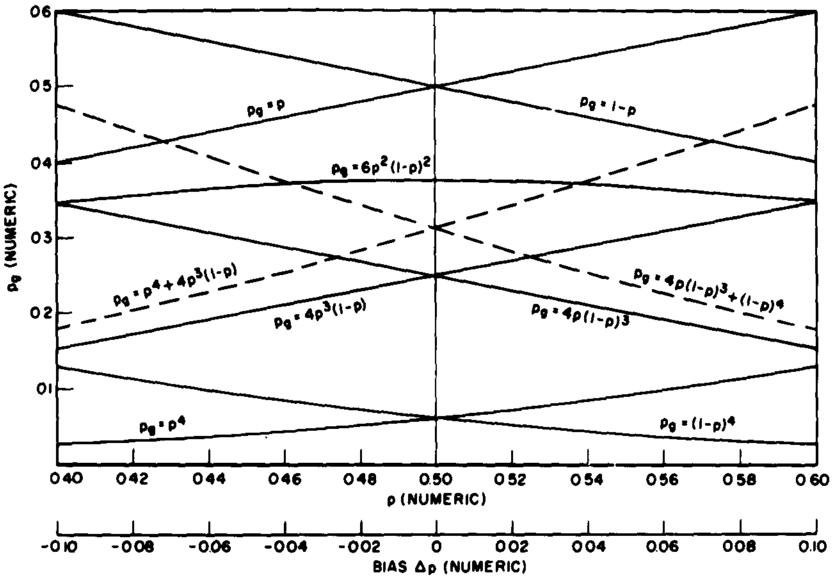


Fig. 4 - Expanded graphical representation of tranformations between p and p_g for some number symbols for m = 1 and m = 4. The two dotted lines show one possible alternate combination of the group probabilities for m = 4.

In (39), since p_g and n (hence, σ as well) are constant, the range of values of k can be obtained. In Fig. 5 the variation in k is shown for seven values of x_k (0, ±1, ±2, and ±3) for each of three values of n (10,100 and 1000). For each set of curves the maximum usable values of x_k are shown. In only the case for n = 10 does the extreme curve (x_k = 3) exceed the limiting condition of (35).

Tolerance Lines

In evaluating (33) it is desirable* to use the limits $x_k \pm h/2$. It follows from (28) that

$$x_{k_1 - 1/2} = (np_{g_1} - 1/2)h = (k_1 - 1/2)h \tag{40a}$$

and

$$x_{k_2 + 1/2} = (np_{g_2} + 1/2)h = (k_2 + 1/2)h. \tag{40b}$$

The values given by (40) will be used in (33).

Having a knowledge of the range of valid values of x_k we can obtain, using (28), the expected range of values of p_g which could be used in determining their contribution to accept readings. Note that the only condition imposed on p_g thus far has been that of constancy. By solving (28) for p_g we obtain, dropping the subscripts of both k and x,

$$p_g = \frac{x^2 + 2k}{2(x^2 + n)} \pm \sqrt{\left[\frac{x^2 + 2k}{2(x^2 + n)}\right]^2 - \frac{k^2}{h(x^2 + n)}}, \tag{41}$$

the range of values of p_g to be expected for given n, k, and x. It is expected that (40) will be used to provide values for x and k for (41). The sign of the radical in (41) is chosen on the basis of the expected value of p_g; there is symmetry, of course, about x = 0.

*W. Feller, op. cit., p. 137.

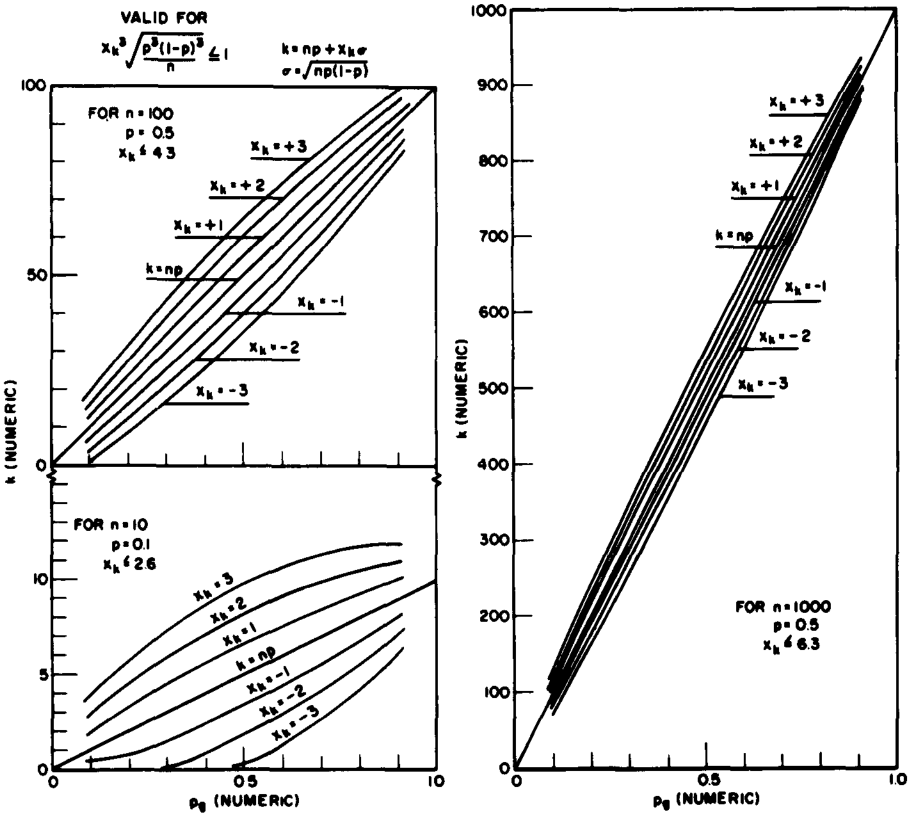


Fig. 5 - Group count (k) as a function of p_g, the probability of occurrence of the particular digital group or number symbol, for n = 10,100,1000, and for x_k = 0, ±1, ±2, and ±3 for each value of n.

A knowledge of the range of valid values of p_g is useful for several reasons. It provides, first of all, a test of the range of significant values over which the probability that counts within the tolerance limits will occur. In addition, the valid regions of p_g for both terms of the right-hand side of (33) can be obtained independently. Furthermore (41) is the basis for a method of comparing different measure functions, as will be shown in the sequence.

By using (41) to calculate at least two points, a straight line can be drawn on arithmetic probability graph paper for each of the terms on the right-hand side of (33); these lines we call tolerance lines. The tolerance lines will be found to be useful in construction of the acceptance characteristic of measure functions, as will be shown.

An Independent Measure System

With the aid of Fig. 5 we have another measuring system. This system yields values of p and consists of obtaining a set of readings. Each reading is obtained from an n by m array. To obtain each reading, a count is made of the frequency of occurrence of the specific arrangement of digits indicated by the selected measure group e.g., (15). By taking a sufficiently large number of readings, calculation of the average value of count will permit the use of Fig. 5 in obtaining the most likely value of p_g (the $x_k = 0$ line is used). Associated with the determination of the most likely value of p_g, there is an indication of the range of variation in count to be expected, and the set of readings can be tested against this variation for consistency.

THE GO/NO-GO MEASURING SYSTEM

While the aforementioned procedure does provide a measuring system, it is not a go/no-go method; an average value must still be calculated. The advantage of a go/no-go method of measurement, in which only counting in involved, lies in the simplicity of interpretation. Any particular reading, when obtained, carries with it an accept or reject classification. This type of classification tends to permit the conclusion that when a "go" or accept classification is obtained, the process is following the model, and the value of p_g is within the tolerance permitted. To assure ourselves of this conclusion, we must examine the expected results more fully. In a go/no-go measuring system, allowable tolerances on p will be set, n will be determined, and the tolerances on k, k_1, and k_2 will be obtained, at least initially.

The Effectiveness of Measure Functions

Equation (41) is of value in the comparison of specific measure functions. For example, one method of comparison might consist of calculating the value of p_g for some "standard" value* of x. By transforming the value of p_g into p, a range of values of p which provide accept readings is obtained. The problem of comparing different measure functions leads us to consider the ideal measuring problem, Fig. 6. The measure area of Fig. 6 is a plot of $M(k_1, k_2, n, p_g)$ vs p. It can be shown that both scales have minimum values of 0 and maximum values of 1. Ideally, an accept region a which is sharply divided from the reject region is desired. We will find in practice a measuring situation more like that shown in Fig. 7, where the lines of demarcation of the accept region are not linear. Note that the extent of the accept region, the p-tolerance region, is ideally $2\Delta p$ or $\Delta p_1 + \Delta p_2$, depending upon whether or not the tolerances are assigned symmetrically. This ideal situation suggests that, in terms of p-tolerances,

$$\left[\frac{d}{dp} M(k_1, k_2, n, p_g)\right]_{p_o - p_1} \sim \infty \text{ and } \left[\frac{d}{dp} M(k_1, k_2, n, p_g)\right]_{p_o + p_2} \sim \infty \tag{42a}$$

or, equivalently, in terms of p_g-tolerances,

$$\left[\frac{d}{dp} M(k_1, k_2, n, p_g)\right]_{p_{g_1}} \sim \infty \text{ and } \left[\frac{d}{dp} M(k_1, k_2, n, p_g)\right]_{p_{g_2}} \sim \infty \tag{42b}$$

where the derivative is evaluated at the values given outside of the brackets. Condition (42) can be expressed more practically as follows: Among alternative measure functions the most effective is that whose slope is greatest at each tolerance limit.

In Fig. 7 the departure from the ideal is indicated by the two cross-hatched regions a_r and r_a. The region a_r is an addition to the accept region and includes values of p outside of the interval of acceptance $(p_o - \Delta p_1, p_o + \Delta p_2)$. The region r_a is an addition to the reject region even though the values of p are within the accept interval. The extent of these two regions in terms of values of p_g can be obtained using (41) for both values of k.

*The choice of a standardized value is quite arbitrary. The value of x which is chosen should be large enough to include a reasonable range of values of p and still be consistent with the validity condition given by (35).

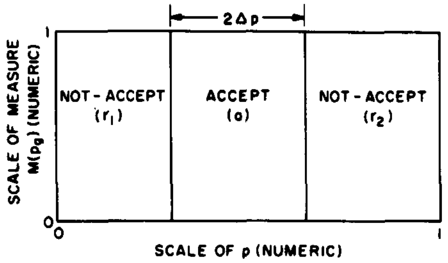
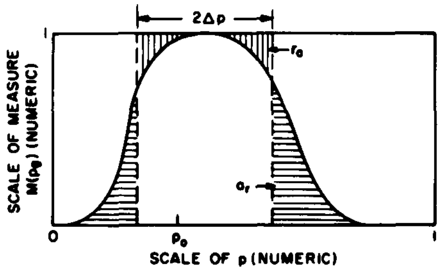


Fig. 6 - The ideal measure area ($M(p_g)$ vs p) with the accept region linearly separated from the reject

Fig. 7 - A typical measure area ($M(p_g)$ vs p) with the accept nonlinearly separated from the reject region. The region a_r is an addition to the accept region and includes values of p outside the interval of acceptance ($p_0 - \Delta p_1$, $p_0 + \Delta p_2$). The region r_a is an addition to the reject region even though the values of p are within the accept interval.



In terms of these areas, condition (42) can be restated as follows: (a) if the value of p to be determined is in the accept interval ($p_0 - \Delta p_1$, $p_0 + \Delta p_2$), the best measuring function is that which gives the smallest area r_a; (b) if the value of p is outside the accept interval, the best measuring function is that which gives the smallest area a_r.

There may be cases where either one of the above two conditions can be satisfied. In other cases a compromise may have to be made. In making the compromise, a measurement of the areas is a quantitative indication of the effect to be expected on the overall measurement. In any event, these areas are of importance in judging the expected effectiveness in the determination to be made of values of p.

If we denote the ideal accept region (Fig. 6) by A, we see that

$$A = 2\Delta p = \Delta p_1 + \Delta p_2 \tag{43}$$

since the ordinate is unity. If we take R to be the rejection region, then, since we have unit measure area,

$$R = 1 - A. \tag{44}$$

From Fig. 7 we have an effective accept region A_e given by

$$A_e = A - r_a + a_r. \tag{45}$$

There is, correspondingly, an effective reject region R_e given by

$$R_e = R - a_r + r_a. \tag{46}$$

From (45) and (46) we can see that if the areas a_r and r_a are made equal we have $A_e = A$ and $R_e = R$. This indicates the best compromise that can be expected. Note that if both tolerances are assigned in accordance with (37), then a "best compromise" results.

We can compare various measure functions on the basis of the capability to give accept indications when the value of p to be determined is within the tolerance interval. We can also make a comparison on the basis of giving reject indications when the value of p being determined is outside of the tolerance interval. We can take E_a as a measure of the acceptance effectiveness, where

$$E_a = \frac{A - r_a}{A} = 1 - \frac{r_a}{A} = 1 - \frac{r_a}{\Delta p_1 + \Delta p_2} \tag{47a}$$

and E_r for the rejection effectiveness, where

$$E_r = \frac{R - a_r}{R} = 1 - \frac{a_r}{R} = 1 - \frac{a_r}{1 - (\Delta p_1 + \Delta p_2)}. \tag{47b}$$

The values E_a and E_r are overall indications covering all values of p either within the tolerance interval or outside of it.

Acceptance Characteristics

In discussing the effectiveness of measure functions, the line of demarcation between the accept and reject regions was considered in a general way. It is possible to obtain data for plotting this line and thereby obtain the accept reject region boundaries. In the case where tolerances on p are given, the characteristic of interest is a plot of $M(k_1, k_2, n, p_g)$ vs p. A plot of this characteristic for each of several possible measure functions will provide a graphical means of comparison.

There are several ways of obtaining data for plotting the accept reject boundary lines, i.e., the acceptance characteristic. Once n is obtained, e.g., from Fig. 2, k_1 and k_2 are obtained from (38). Then either (18) or (33) can be used. Calculations using (18) or (32) can be made either directly, or tables* can be used. If tables are used, there is a restriction on values of n; the tabulation* used includes values of n up to 1,000.

The use of (33) with due regard for its range of application provides a practical means of getting the data for acceptance characteristics. In fact, the two terms on the right-hand side of (33) can be treated independently. It is necessary to treat them separately if gross errors resulting from failure to satisfy condition (36) are to be avoided. That gross errors can be avoided becomes evident once it is considered that (32) and (33) both attain the values 0 and 1 for finite values of x. It is possible to use arithmetic probability graph paper to get a reasonably approximate acceptance characteristic. In this case, with p_g plotted as the abscissa, a straight line can be drawn connecting the selected points. The actual characteristic as a function of p can then be obtained graphically.

The advantage of a graphical method lies in the ease with which adjustments can be made in the limits initially chosen. The comparative effect on the measuring effectiveness can be seen by plotting the initial and subsequent limit lines.

The acceptance characteristic yields at least a qualitative judgment of the measuring effectiveness of specific measuring functions. If the p-tolerance lines are drawn in and the appropriate areas are measured, then there is a quantitative judgement. In the measuring case where p is obtained from Fig. 5, the probable range of variation to be expected in k is obtained directly from Fig. 5. In the go/no-go case, a point on the acceptance characteristic gives the probability of acceptance for the particualr value of p. The area

*"Tables of the Cumulative Binomial Probability Function," by the Staff of the Computational Laboratory, Harvard U. Press, 1955.

under the acceptance characteristic represents the probability of acceptance for all values of p. The effective accept region given by (45) is the probability that if the value of p being measured is within the tolerance limits for p, an accept indication will be obtained.

From Fig. 7 we see that the probability of acceptance decreases as we increase or decrease p with respect to the central value p_o. We must take this variation into account in interpreting the readings of a go/no-go measuring system.

Effect of Repeated Measurements with a Decision Criterion

In a go/no-go measuring system, the value of p is not obtained. Instead, the measurement indicates that a particular value of p is essentially within the p-tolerance interval. In such a system, the acceptance characteristic gives the probability of acceptance for any particular value of p. The value of the probability of acceptance remains constant as long as p remains constant. Thus, a pseudorandom digit generator which is stable will be expected to yield a value of p which remains substantially constant. If for some reason a change in p occurs, then there is a corresponding change in the probability of acceptance. If the value of p was initially near the central value, then the probability of acceptance would decrease or the probability of rejection would increase. Now, we can choose to use either the probability of acceptance or of rejection as the constant probability in a new sequence of repeated trials. Let there be n_s trials with the constant probability p_s (i.e., the probability of acceptance) in each trial. We use a small value for n_s and assign a value to k_d, the number of acceptable occurrences out of n_s trials. The expectation that out of n_s trials there will be at least k_d occurrences when the constant probability of acceptable occurrence in a single trial is p_s, is given by

$$B(n_s, k_d, p_s) = \sum_{x=k_d}^{n_s} n_s \, p_s^x \, (1 - p_s)^{n_s - x} \tag{48}$$

The probability $B(n_s, k_d, p_s)$ is tabulated; it is the cumulative binomial probability function referred to earlier. The selection of n_s and k_d is quite arbitrary. For purposes of illustration let us take some small number such as $n_s = 10$. With the aid of tables, k_d might be so chosen as to make

$$B(n_s, k_d, p_s) \geq 0.50, \text{ when } p_s = 0.50 . \tag{49}$$

This choice of p_s follows from the way in which k_1 and k_2 were selected (by (38)). The result from the tables gives $k_d = 5$ and $B(n_s, k_d, p_s) = 0.62$.

By introducing (48), we are provided with a means of interpreting a series of readings; in short, we have an acceptance decision criterion. With its aid we can predict the increase in rejection rate as the value of p departs from the central value. To illustrate a possible use of this type of decision criterion, the function (48) has been plotted, with the aid of tables for four values of k_d (Fig. 8). Since the values of k_1 and k_2 were set essentially to give a probability of acceptance of 50 percent, if we use (49) as the decision criterion then whenever p approaches one of its tolerances it can be expected that there will be only about 5 acceptance readings in 10 trials. From Fig. 8 with p_s = 0.5, we could expect a variation in the number of acceptances of between at least 4 and 7, and the process under test would still be following the model.

Repetitive Patterns

The go/no-go measurement of randomness in a system which has no memory involves the risk of accepting sequences which are repetitive. The very fact that a given randomness generator begins to produce sequences of digits which are repetitive is an indication

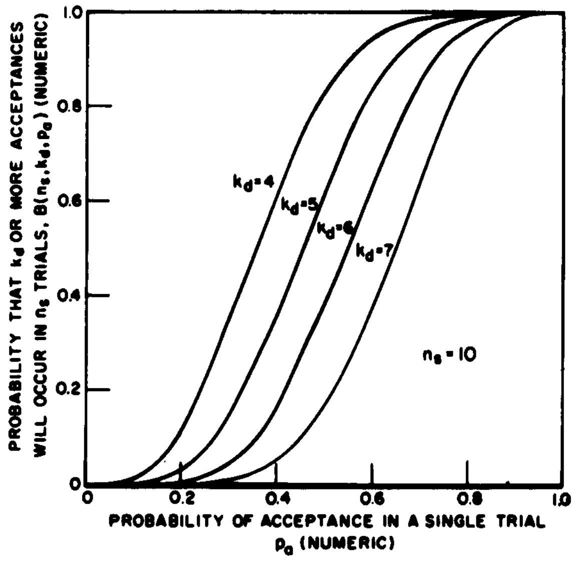


Fig. 8 - Acceptance criterion $[B(n_s,k_d, p_a)]$ vs the probability of acceptance for four values of k_d

of failure of the generator to perform properly. Thus, it is the capability of the measuring system to detect certain types of generator failure that we are investigating at the moment. In specific cases, a generator may produce only certain sequences, so with these known, the measuring system should be designed to cope with those sequences, i.e., to give reject indications when they do occur. Here we point out a few of the general aspects of the problem.

The problem of determining the effect of repeated sequences is treated in detail in Appendix C. It is shown that the investigation is tedious and no general method of making the test is evident.

It is possible to make the following qualitative generalizations from the investigation made in Appendix C.

(a) The vulnerability of measure functions to erroneous accept indications depends upon the choices made for m (i.e., the specific measure groups resulting when p_g is designated), as well as upon the values of k_1 and k_2.

(b) While some reduction in vulnerability to accept indications is possible through a narrowing of the acceptance limits, the change in the acceptance characteristic should be determined.

(c) The use of a decision process (e.g., multiple application of a measure function) should reduce the probability of erroneous acceptance indication and, therefore, the vulnerability.

(d) It should be possible to reduce vulnerability by the use of two or more measure functions which individually have different regions of vulnerability.

That the incidence of repetitive sequences is a departure from the ideal can be seen if the probability of occurrence of specific sequences is considered. A sequence of m_s repeated digits can be expected to occur with a probability p_s in such a way that in the ideal case of $p = 0.5$

$$p_s = 2^{-(m_s)}. \tag{50}$$

In other words, each of the possible arrangements is equally likely. We can obtain from tables the probability that for a given m_s a specific grouping would occur continually in an ideal process. These values have been tabulated (Table 1). It can be seen that for $m_s = 1$, the probability that there will be a sequence as long as 8 digits is quite small; we should never expect to find as many as 18 digits repeated. In the same way we find that we should encounter almost no occurrences of sequences where $m_s = 7$.

Table 1
The Probabilities of a Specific Sequence of m_s Digits Occurring Each Time in n Trials for an Ideal Binary Process

m_s	$2m_s$	$1/2^{m_s} = p_s$	Probability That the m_s Digits Will Be Repeated Each Time in n Trials						
			Number of Trials (n)						
			2	3	4	5	6	7	8
1	2	0.5	0.25	0.125	0.0625	0.03125	0.01563	0.00781	0.00391
2	4	0.25	0.06250	0.01563	0.00391	0.00098	0.00024	0.00006	0.00002
3	8	0.125	0.01563	0.00195	0.00024	0.00003	0.00000		
4	16	0.0625	0.00391	0.00024	0.00002	0.00000			
5	32	0.03	0.00090	0.00003	0.00000				
7	128	0.01	0.00010	0.00000					

It follows that in choosing a value of m, consideration should be given to making it as near to 7 as possible. Of course, the complexity of testing is undoubtedly also directly dependent upon m. A balance must be struck between vulnerability and complexity. In devising the entire test, consideration might be given to the use of at least one measure function for which $m = 7$, and this should be a direct indicator of erroneous accept indications from repeated sequences.

APPLICATION OF THEORY

We are ready to consider an example to illustrate the procedure for applying the theory developed above. A rather arbitrary case is being used to eliminate the need for special consideration which might be required in initially setting the p-tolerances. Thus, instead of starting with given p-tolerances, a nominal value of $p_0 = 0.5$ was chosen. The lower and upper limits, Δp_1 and Δp_2, were then selected individually from a shuffled "deck" of cards. The values obtained are

$$\Delta p_1 = 0.062 \text{ and } \Delta p_2 = +0.038.$$

It follows that the p-tolerances are 0.438, the lower limit, and 0.538, the upper limit.

We will examine the following three measure groups as part of the demonstration of the theory: p, $6p^2q^2$, and $p^4 + 4p^3q$. Next we make the assumption that an error of 5 percent or less is permissible. We find from Fig. 2 that a sample size n of about 1,000 is required. We note that condition (26), when evaluated, gives $n\epsilon^3 = 0.125$, a value considered close to zero and satisfying (35) as well. We should, therefore, expect a reasonable approximation of the binomial distribution using the normal law equivalent.

In Appendix B it has been shown that a good indication of the upper bound of the error in p_g can be obtained from Fig. 2, and that the error in p can be within this bound. In Appendix B the three specific groupings selected for our discussion have been evaluated with regard to the error in p. For $p_g = p$, the error in p is just the error in p_g. For $p_g = 6p^2q^2$, the relative error in p has an asymptote at $p = 0.5$. For $p_g = p^4 + 4p^3q$, the asymptote for the relative error in p occurs at $p = 1$. Since the asymptote for $p_g = 6p^2q^2$ occurs at $p = 0.5$, which is within the region of measuring interest, we would suspect that that particular grouping might not be suitable. This turns out to be the case for other reasons as well. Because this function has some interesting qualities it will be treated further. The relative error in p for $p_g = p^4 + 4p^3q$ is less than the relative error in p_g over a wide range of values of p, including the region of interest between 0.438 and 0.538.

Graphically Determined Acceptance Characteristics

Using (38) we can obtain values for k_1 and k_2. At this point we can use graphical techniques in obtaining the acceptance characteristics. By selecting at least two values for x_k and using (41), points are obtained to make a straight-line estimate of the acceptance characteristic when plotted on arithmetic probability graph paper. By plotting the tolerances separately, the difference indicated by (33) can be obtained graphically from the two straight-line plots on the graph paper itself. This was actually done, and Figs. 9-12 are the result. To illustrate the degree of agreement possible, points on the acceptance characteristics were obtained using data from a table of the cumulative binomial function.* In Figs. 9, 10, and 12, the straight lines are adjudged to be a reasonable connection of the triangularly designated points. The circularly designated points were obtained from the table of the cumulative binomial function. Because the measure group $6p^2q^2$ (Fig. 11) exhibits some interesting qualities for the tolerances which were obtained, it was decided to plot the composite or acceptance characteristic curve by calculating a number of points, indicated by crosses, using (33) directly. In Fig. 11, the curve which has been drawn was obtained graphically from Fig. 10, and the crosses and circles are points obtained, respectively, from (33) and (32). Further evidence of the agreement obtainable is shown in Fig. 12; the same designations for points applies as in Fig. 11.

We note from Fig. 11 that the two lines corresponding to the distributions about the two tolerances are both incomplete and close together. The terminal point of the two lines corresponds to the maximum value of

$$p_g = 6p^2q^2$$

which occurs for $p = 0.5$. The two lines are close together because p_g is symmetrical about $p = 0.5$; there are two values of p for each value of p_g. In case this particular function is to be used in determining values of p, ambiguities will arise, and other means have to be used to resolve the ambiguity.

With the aid of Figs. 3 and 4, values of p_g can be transformed into values of p. Then the curves of Figs. 9, 11, and 12 can be used to obtain acceptance characteristics for each of the measure groups, Figs. 13-15. The acceptance characteristic is a plot, on linear scales, of the probability that the specific measure groups occur for particular values of p when n and k are fixed. Again, to indicate the effect of the normal law approximation, a comparison is made with results obtained using the table of the cumulative binomial probability function.

*The staff of the computational laboratory, Harvard University, op. cit.

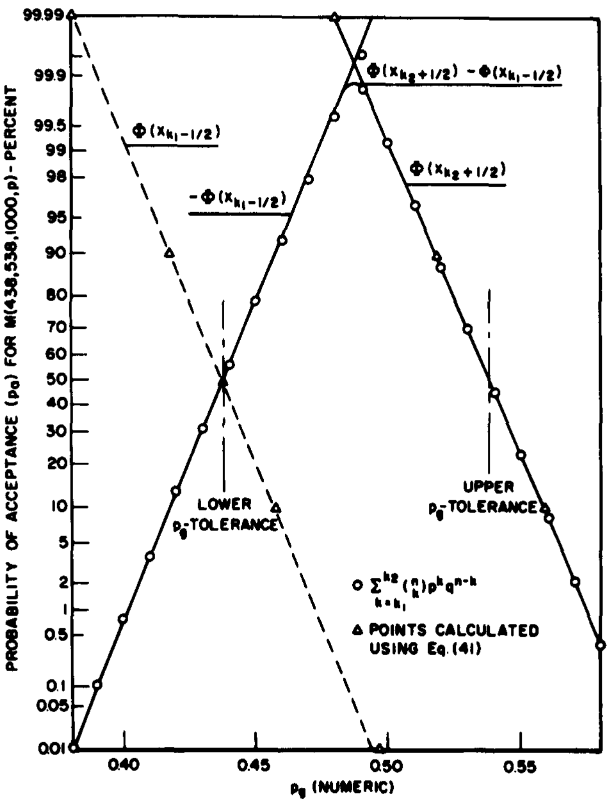


Fig. 9 - Tolerance lines (acceptance characteristics) for the measure function M(438,538,1000,p). The straight lines join points calculated by Eq.(41). Note that the points calculated by the cumulative binomial function lie on these straight lines also. The values $-\Phi(x_{k_1} - ½)$ are: one minus the left-hand scale reading.

Fig. 10 - Tolerance lines (acceptance characteristics) for the measure function M(363,372,1000,6p²q²)

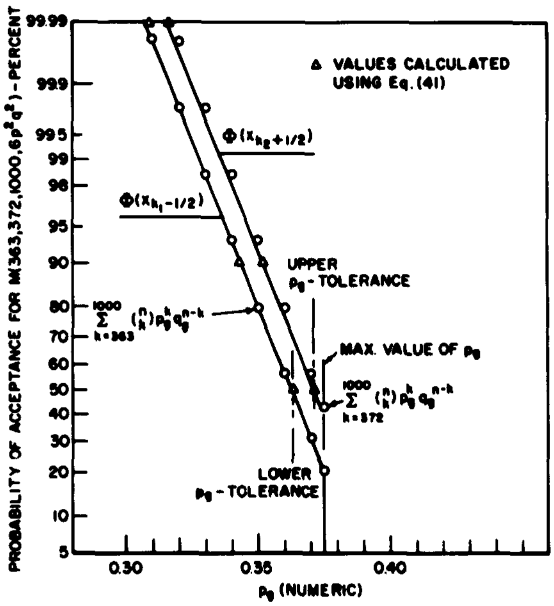
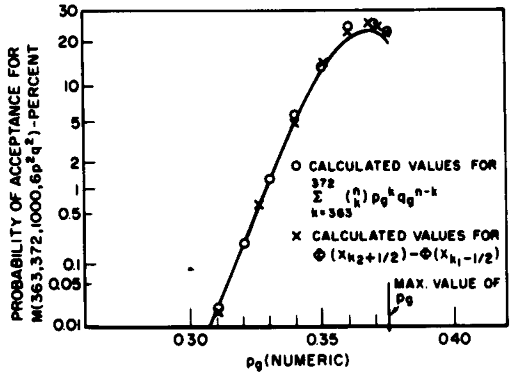


Fig. 11 - Graphical composite (solid curve) of tolerance lines shown in Fig. 10. The values calculated by the cumulative binomial function (circled points) are shown for comparison.



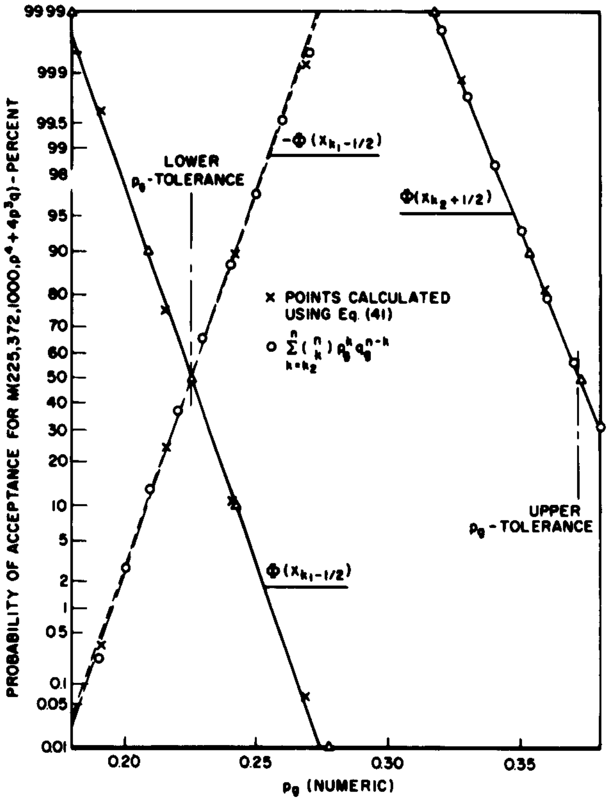


Fig. 12 - Tolerance lines (acceptance characteristics (for the measure function M(225,372,1000,p^4 + $4p^3q$). The values for $-\Phi$ $(x_{k_1}$ - ½) are: one minus the left-hand scale reading.

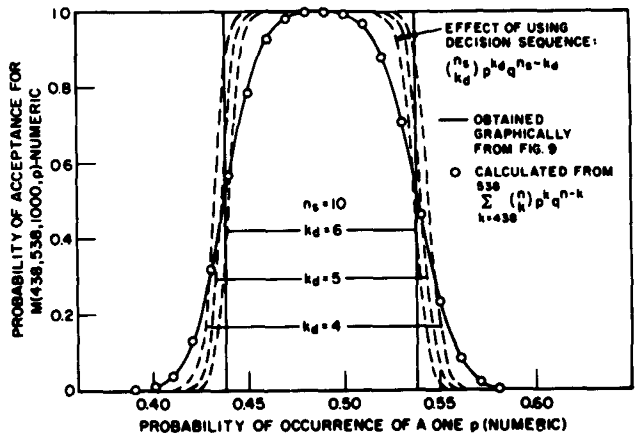


Fig. 13 - Acceptance characteristic for the measure function M(438,538,1000,p) (solid curve) obtained graphically from Fig. 9. Comparison with three decision sequences, as indicated.

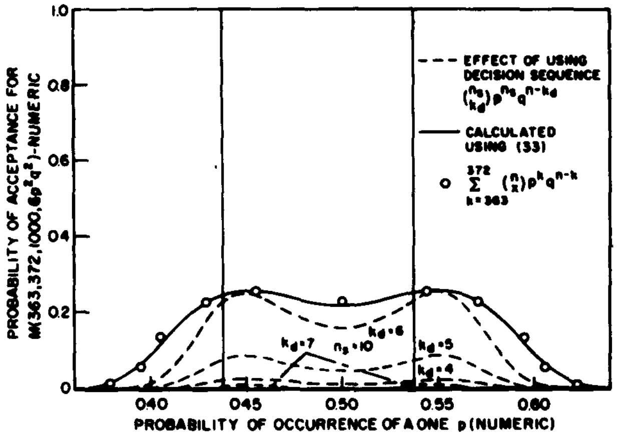


Fig. 14 - Acceptance characteristic for the measure function M(363,372,1000,6p^2q^2) (solid curve) based on Eq. (33). Comparison with four decision sequences, as indicated.

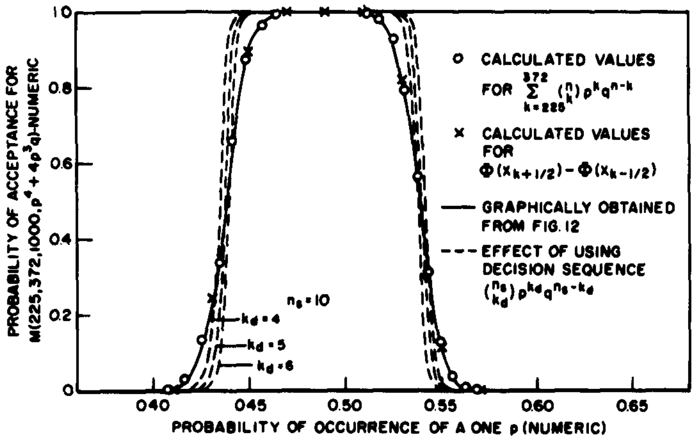


Fig. 15 - Acceptance characteristic for the measure function M(225,372,1000,$p^4 + 4p^3q$) (solid curve) obtained graphically from Fig. 12. Comparison with three decision sequences, as indicated.

Effect on Acceptance Characteristics of Repeated Measurements and a Decision Criterion

Having obtained the acceptance characteristics, the effect of using an acceptance decision criterion, such as that given by (48), can be determined. The acceptance characteristics gives, for specific values of p, the probability of acceptance in a single trial as the ordinate in Figs. 13-15. Figure 8 is a plot of the probability that there will be k_d or more occurrences of specific groups of digits (the ordinate) as a function of the probability of acceptance in a single trial (the abscissa). We can use graphical means to obtain new characteristics: the probability that there will be k_d or more acceptances in $n_s = 10$ independent trials. To show what such characteristics look like and to indicate the variation to be expected, three values of k_d (4, 5, and 6) were selected. The results are superimposed on the acceptance characteristics, Figs. 13-15. The increase in sharpness is apparent. In Fig. 14, four values of k_d were used to show the complete trend as k_d is increased.

The increase in sharpness of the acceptance characteristics indicates that the theoretical line of demarcation between the accept and reject regions of the measure area can be approached quite closely. Thus, conditions (42) can be satisfied and the effectiveness given by (47) should be of high order.

From Figs. 13-15 not only is the increased sharpness shown, but the usefulness of criterion (49) is indicated.

Comparison of Figs. 13, 14, and 15 shows that two of the functions yield similar acceptance characteristics. The second, $p_g = 6p^2q^2$, however, yields a different characteristic. In terms of (47) it can be stated qualitatively that the second function does not offer very good acceptance effectiveness for the tolerances chosen. By increasing both tolerances, the tolerance lines become separated and the acceptance characteristic can be made to reach unity.

Use of Graphical Means for Adjusting Tolerances

As a demonstration of the usefulness of the graphical method in the adjustment of tolerances, we consider the grouping $p_g = 6p^2q^2$ further. With reference to Fig. 16, an initial change in tolerances was made by changing k_1 radically to 265, while changing k_2 only slightly to 375. Using (41), calculations yield the points for drawing the straight line, indicated by the triangles. In this case the lower tolerance was obtained, using (40), after the extreme value had been obtained for the case where $k_2 = 375$. This choice assured no crossover of the tolerance lines (see Fig. 16). This choice of tolerances still gives a depressed central region up to the point where the upper limit line crosses the line of maximum value of p_g, 0.375. To remove the depressed region it is necessary to increase the upper limit further. A clue to the amount of increase is obtained from Fig. 5 ($n = 1000$): it is found that for this particular function, when at its maximum value, readings (i.e., values of k) up to about 430 are still quite probable. However, an arbitrary decision was made to accept values of k of about 410 with $1 < x_k < 2$. At this point it was observed from the plots of the first revised tolerances that the slope of the two lines is nearly the same. By sketching in on a worksheet the new line, an attempt was made to find the lower limit graphically. Here, it was only necessary to go far enough with the lower limit line to permit a small amount of crossover. Thus, it was found that a value of about 310 could be used. It was decided to compare these lines with the lines which would be obtained for other comparable values – hence, the lines for $k_1 = 302$ and $k_2 = 400$. To show the results of the graphical process, points for each of the lines mentioned were calculated using (41). Note that in the case of the last two upper limit lines it was necessary to plot points which have only graphical significance since they are beyond the maximum value of p_g.

To illustrate the effect of choosing the various tolerances on the actual acceptance characteristics, two of the sets of tolerances referred to in the description of the graphical process have been plotted (Fig. 17) along with the previously obtained acceptance characteristic. From Fig. 17 it can be seen that the increase in acceptance effectiveness is obtained at a sacrifice in rejection effectiveness.

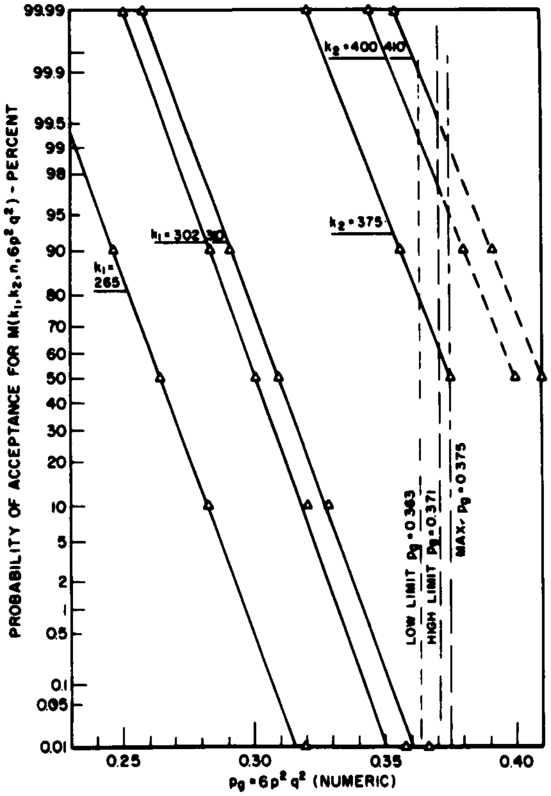


Fig. 16 - Tolerance line adjustments obtained by changing k_2 and k_1 for the measure function $M(k_1, k_2, 1000, 6p^2q^2)$

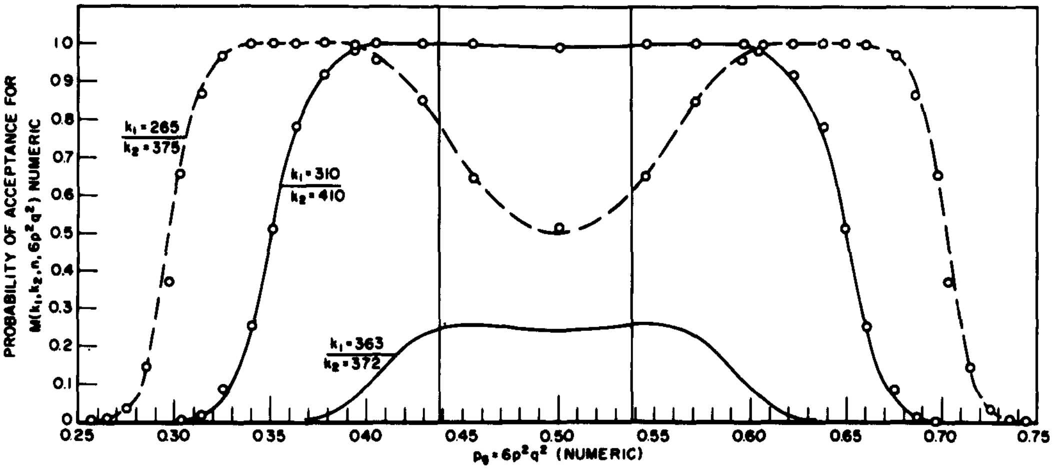


Fig. 17 - Effect of choosing various tolerances (values of k_1 and k_2) on the acceptance characteristic of $M(k_1, k_2, 1000, 6p^2q^2)$

Application of Graphical Means in Comparing Measure Functions

The success of graphical means suggests the possibility of using these results as a rough indication of acceptance and rejection effectiveness. Such an indicator is useful in comparing results to be expected with the various measure functions. From Figs. 9, 10, 12, and 16 the upper limit on nearly each of the tolerance lines is coincident with the calculated point; the end of the probability graph paper yields a useful, although arbitrary, range of the characteristic. This choice offers a useful standard point of reference. In this kind of indication, two factors are of significance: (a) the value of the measure function at the point of intersection of the tolerance line with the p-tolerance value, and (b) the range of values of p out to the significant end of the tolerance line. These two factors outline standardized portions of the regions r_a and a_r in Fig. 7.

Following the foregoing method, two sets of values are given in Table 2: those for the acceptance region (indicating the extent to which desired values of p are rejected) and those for the rejection region (indicating the extent to which undesired values of p are accepted). There are limitations in the use of the data of Table 2. While the first entry for the acceptance region is straightforward, the second entry contains a dash. This dash must be interpreted as a failure of the tolerance line to reach the end of the graph paper. Another difficulty arises because there is a depression in the acceptance characteristic within the acceptance region. This situation is handled by introducing the middle category. The point-of-intersection entry in the middle category indicates the lowest point reached by the depressed portion of the characteristic; in the cases tabulated, the region affected by the depression in the acceptance characteristic is included between the two p-tolerances. Aside from these special interpretations the data can be used in comparing different measure functions. From the tabulation we find that of the three functions, the function $M(225,372,1000,p^4 + 4p^3q)$ has the smallest areas r_a and a_r, and these two areas are of approximately the same size. Hence, this function most nearly satisfies (42) and should give the best overall acceptance characteristic.

Vulnerability of Measure Functions to Erroneous Accept Indications

Having obtained a rough comparison of the three measure functions being used in this application, it is necessary to make some comparison of the capability for each of these functions to reject certain known repetitive sequences. The sequences have been examined in Appendix C.

Table 2
Evaluation of Acceptance Characteristics from Tolerance Line Measurements

Region	Measure Function	Lower		Middle	Upper		Remarks
		Point of Intersection	Range (p-Scale)	Point of Intersection	Point of Intersection	Range	
Acceptance	$M(438,538,1000,p)$	0.51	0.056	0.9988	0.51	0.058	Data from Fig. 9
	$M(363,372,1000,6p^2q^2)$	0.51	-	0.21	0.51	-	Data from Fig. 10
	$M(265,375,1000,6p^2q^2)$	< 0.0001	0	0.51	<0.0001	0	Data from Fig. 16
	$M(310,410,1000,6p^2q^2)$	<0.0001	0	0.991	<0.0001	0	Data from Fig. 16
	$M(225,372,1000,p^4 + 4p^3q)$	0.51	0.035		0.51	0.031	Data from Fig. 12
Rejection	$M(438,538,1000,p)$	0.51	0.058		0.51	0.059	Data from Fig. 9
	$M(363,372,1000,6p^2q^2)$	0.51	0.088		0.51	0.102	Data from Fig. 10
	$M(265,375,1000,6p^2q^2)$	<0.0001	0.188		<0.0001	0.212	Data from Fig. 16
	$M(310,410,1000,6p^2q^2)$	<0.0001	0.148		<0.0001	0.172	Data from Fig. 16
	$M(225,372,1000,p^4 + 4p^3q)$	0.51	0.038		0.51	0.034	Data from Fig. 12

In Appendix C two methods of sampling sequences made up of repeated groups of digits are used. The results of the investigation of Appendix C are plotted in Fig. 18. For both sampling methods the probability of acceptance for each of 184 sequences has been obtained. In Fig. 18 this probability of acceptance for each of the 184 sequences, and for the three measure functions being considered here for purposes of illustration, has been plotted.

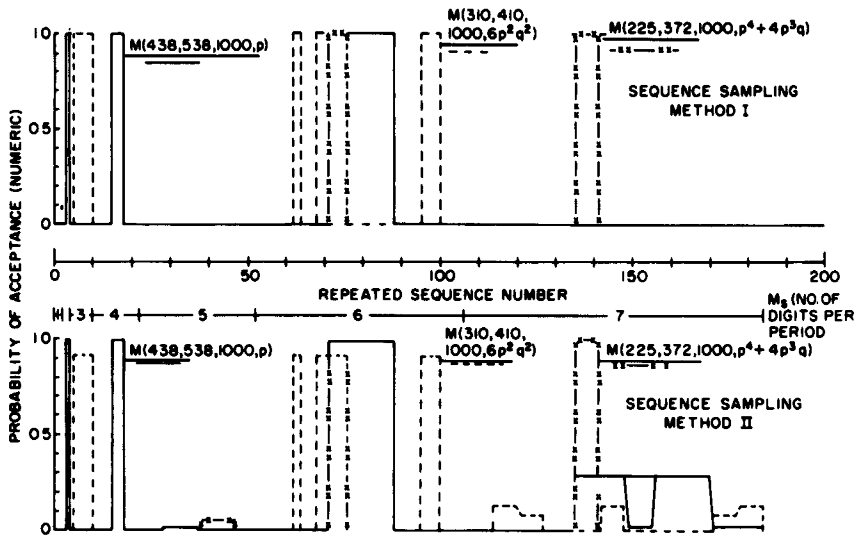


Fig. 18 - Effect of repeated sequences on three measure functions

Aside from the fact that sampling method II (see Fig. 18) yields acceptance indications from more sequences, but with generally lower probabilities, the individual vulnerability of the measure functions increases in the following order:

$$M(438,538,1000,p)$$

$$M(310,410,1000,6p^2q^2)$$

$$M(225,372,1000,p^4 + 4p^3q).$$

For the measure functions being considered, m is equal to 1 in the first function and to 4 in the other two functions. From Fig. 18, the first erroneous indications for the more stringent method II occur respectively at $m_s = 2$, 3, and 5, the measure functions being considered individually. If, however, the third measure functions is combined with either of the first two measure functions, the only common region of erroneous acceptance indication occurs for $m_s = 6$. This represents some increase in the fidelity of go/no-go accept indications.

From Fig. 18 we see that for the case in which two measure functions are combined, there are seven sequences which will cause erroneous accept indications. A further increase in the fidelity of accept indications should be obtained by determining the measure function which includes just the 7 sequences which cause the erroneous accept indications.

For the illustrative example being considered, a satisfactory go/no-go measuring system consists in using three measure functions, $M(438,538,1000,p)$, $M(310,410,1000,6p^2q^2)$, and $M(225,372,1000,p^4 + 4p^3q)$, on which the limits and acceptance characteristic have not been determined but which includes the seven sequences which cause the erroneous accept indications.

SUMMARY AND CONCLUSIONS

The general problem of testing a particular process for randomness reduces to the problem of examining a sequence of numbers to determine that the set of numbers have statistical characteristics which are within predictable limits. The sequence or set of numbers can be arranged into an n by m array. The dimensions of the array yield certain information about the tests which might be performed to determine the randomness of the numbers contained in the array. The length n (number of rows) of the array sets the upper bound on the measuring error (in the value of p), whereas the width m (number of columns) is an indicator of the digital groupings which can be used for randomness testing. The width m of the array serves also (for go/no-go tests) as an indicator of the capability of specific digital groups to reject nonrandom sequences (i.e., groups of digits which are repeated) and thereby to prevent false (go) indications.

Consider the case of an array of binary digits. If the assumptions are made that each entry in the array is independent of any other entry, and the probabilities of generating the two digits remains constant, then the array could have been generated from Bernoulli trials. Thus the binomial distribution and its characteristics serve as the theoretical basis of comparison for observed results.

It has been shown that there are many kinds of tests which can be devised to measure randomness. Essentially these are tests in which p is measured indirectly, by using any term or combination of terms in the binomial expansions $[p + (1 - p)]^m$. In selecting a particular value for m, an effective transformation in the array is made, from a m-column array to a single column array, and this is tantamount to a change in number system of higher order radix; the original number system radix is 2. Thus the selection of m is made partly on the basis of the digital group or groups of digits considered of interest.

Although exhaustive testing for randomness is indicated, this investigation has considered the results to be expected from single tests and for tests repeated a small number of times. The investigation was directed to automatic tests, with go/no-go indication. Because the binomial distribution is not as well tabulated as is the normal distribution, the theory was developed about the latter.

It has also been shown, particularly for the go/no-go measuring case, that the choice of the value of m depends upon the desired capability for the test to reject repeated sequences of digits. A value, $m = 5$ or 6, satisfies this requirement if the two means used to generate repeated sequences are the only ones to be considered. The mere choice of a value for m does not prevent repeated sequences, when they occur, from causing false "go" indications. Once m has been selected, various digital groups can be tested to determine which repeated sequences are likely to cause the false indications. It should be noted that m should be given as large a value as possible, and if it is an odd number, the resulting effect of repeated sequences should be minimized. With m an odd number, repeated sequences which might cause false indications should be irregular; hence, it may be easier to devise tests to prevent such false indications. Thus combinations of tests are implied to cope with the problem of false indications. On the other hand, the method of generating the random digits, which essentially is being tested, might profitably be examined to determine if particular sequences are likely to be generated. A particular generator may be prone to fall into a particular pattern or sequence of digits, and this pattern, if known, serves to evaluate the need for concern about repeated sequences when devising the tests. Indeed, it may be impossible for some generators to change from a random to a nonrandom (repeated sequence) state without the test detecting the transition. While there is no unique solution to the problem of selecting the value of m, these are the considerations which must be given. Once the selection of m has been made, the possible digital groups made available for the tests should be checked to determine their effectiveness in measuring p; an error analysis in accordance with Appendix B is required to avoid gross errors. Means are given for determining the upper bound on the error to be expected in measuring p. While this error is primarily determined when the length of the array of the sample size (n) is selected, the error analysis for particular digital groups will show what departures from the upper bound of error can be expected.

Having determined both the particular digital group(s) and n, with known limits for p, the tolerances k_1 and k_2 on the group count can be assigned. The measure function thus obtained is of the form $M(k_1,k_2,n,p_g)$. The effectiveness of particular measure functions can be determined qualitatively once the acceptance characteristic is obtained. An acceptance characteristic is a graph of $M(k_1,k_2,n,p_g)$ vs p. Any acceptance limit line can be compared with the ideal, a straight line of infinite slope. In practice, there will be a small number of measure functions to be compared, and the best measure function will be that having the smallest dispersion of both limit lines.

The acceptance characteristic is essentially composed of two normal distributions, corresponding to the upper and lower limits of p. Because of this fact, acceptance characteristics are readily obtained with the aid of tables of the normal distribution function. With the aid of normal probability graph paper it is possible to obtain the characteristic graphically.

The acceptance of the measure function establishes the results which can be expected in a single go/no-go test. The acceptance characteristic of any measure function can be made to approximate the ideal more nearly by using a relatively small number of tests and adopting a decision criterion. It is shown that considerable improvement is achieved if a sequence of 10 tests is used, with a decision to accept based on 5 acceptances out of 10.

It has been shown that dynamic, automatic testing of randomness can be achieved with useful results. The requirement for a relatively small digital group, to avoid false "go" indications, and for a relatively small number of repeated tests suggests that practical devices can be built to perform the tests.

In developing the theory, a means for measuring p more directly was described. This alternative method consists of obtaining statistically suitable samples, each of size n, of the frequency of occurrence (or count) of specific groups of digits. If enough samples are obtained, the parameters of the distribution of count can be calculated. It can therefore be determined statistically that the counts are distributed randomly. Furthermore, from the average value of the count the most probable value of the group frequency of occurrence can be calculated. The value of p can thus be measured. By the application of this method, an independent check is available for verifying the results of go/no-go tests. The advantage of this alternative method lies in the fact that the instrumentation requirements may be somewhat less than for the go/no-go method.

APPENDIX A

SOME RELATIONS BETWEEN EXPRESSIONS FOR THE NORMAL DISTRIBUTION FUNCTION

Given the normal density function

$$\phi(t) = \frac{1}{(2\pi)^{1/2}} e^{-(t^2/2)}, \tag{A1}$$

the normal distribution function is defined as

$$\Phi(x) = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^{x} e^{-(t^2/2)} \, dt. \tag{A2}$$

Furthermore,

$$\int_{-\infty}^{+\infty} \phi(t) \, dt = \frac{1}{(2\pi)^{1/2}} \int_{-\infty}^{+\infty} e^{-(t^2/2)} \, dt = 1. \tag{A3}$$

We can divide (A3) into three parts:

$$\int_{-\infty}^{-x} \phi(t) \, dt + \int_{-x}^{x} \phi(t) \, dt + \int_{x}^{\infty} \phi(t) \, dt = 1. \tag{A4}$$

Since we are dealing with the normal density function, which is symmetrical about $t = 0$,

$$\int_{-\infty}^{-x} \phi(t) \, dt = \int_{x}^{\infty} \phi(t) \, dt. \tag{A5}$$

It follows that

$$\int_{-\infty}^{-x} \phi(t) \, dt + \int_{x}^{\infty} \phi(t) \, dt = 2 \int_{x}^{\infty} \phi(t) \, dt \tag{A6}$$

$$= 2 \int_{-\infty}^{-x} \phi(t) \, dt. \tag{A7}$$

Using this result in (A4) we obtain

$$2\int_{-\infty}^{-x} \phi(t)\,dt = 1 - \int_{-x}^{x} \phi(t)\,dt. \tag{A8}$$

Let

$$\Phi(x) = \int_{-\infty}^{x} \phi(t)\,dt. \tag{A9}$$

Then

$$\Phi(x) = \int_{-\infty}^{-x} \phi(t)\,dt + \int_{-x}^{x} \phi(t)\,dt. \tag{A10}$$

Also,

$$\Phi(-x) = \int_{-\infty}^{-x} \phi(t)\,dt. \tag{A11}$$

Now

$$\Phi(x) + \Phi(-x) = \int_{-\infty}^{-x} \phi(t)\,dt + \int_{-x}^{x} \phi(t)\,dt + \int_{-\infty}^{-x} \phi(t)\,dt.$$

Using (A5)

$$\Phi(x) + \Phi(-x) = \int_{-\infty}^{-x} \phi(t)\,dt + \int_{-x}^{x} \phi(t)\,dt + \int_{x}^{\infty} \phi(t)\,dt = 1.$$

Therefore,

$$\Phi(-x) = 1 - \Phi(x). \tag{A12}$$

Now take the difference between (A10) and (A11):

$$\Phi(x) - \Phi(-x) = \int_{-\infty}^{-x} \phi(t)\,dt + \int_{-x}^{x} \phi(t)\,dt - \int_{-\infty}^{-x} \phi(t)\,dt$$

$$= \int_{-\infty}^{x} \phi(t)\,dt - \int_{-\infty}^{-x} \phi(t)\,dt \quad \text{(using (A9))}.$$

Therefore,

$$\Phi(x) - \Phi(-x) = \int_{-x}^{x} \phi(t)\,dt. \tag{A13}$$

But, using (A12),

$$\Phi(x) - [1 - \Phi(x)] = \int_{-x}^{x} \phi(t)\,dt$$

or

$$2\Phi(x) - 1 = \int_{-x}^{x} \phi(t)\,dt$$

or

$$\Phi(x) = \tfrac{1}{2} + \tfrac{1}{2} \int_{-x}^{x} \phi(t)\,dt. \tag{A14}$$

Also,

$$\Phi(-x) = \tfrac{1}{2} - \tfrac{1}{2} \int_{-x}^{x} \phi(t)\,dt. \tag{A15}$$

Many sets of tables of the normal distribution function are available. A rather complete one ("Tables of the Probability Functions," Vol. II, FWA, WPA for the City of New York, 1942) tabulates the function

$$\int_{-x}^{x} \phi(t)\,dt.$$

APPENDIX B

THE RELATION BETWEEN THE ERRORS IN p_g AND p.

The ability to select an upper bound to the error expected in making a measurement is of considerable significance. Equation (19) provides a mean for selecting an upper bound to the error in measuring p_g, the probability of occurrence of a specific grouping of digits whose functional relationship may be one or more of the terms in (12). Use of p_g in setting the upper bound of error provides a general way of setting the error, but it does not show how this error affects the value of p, the independent variable in functions represented by p_g.

It has been shown that there are a large number of possible functions of p which can be used to define p_g. We will consider a small number here to show the relationship between the error in p_g, which can be selected by (19), and the corresponding error in p.

In general,

$$p_g = f(p). \tag{B1}$$

Let us differentiate (B1):

$$\frac{dp_g}{dp} = f'(p). \tag{B2}$$

Now, suppose we let the differentials dp_g and dp approximate the respective differences Δp_g and Δp. Substituting the differences for the differentials in (B2) we obtain

$$\Delta p_g \sim f'(p)\ \Delta p \tag{B3}$$

where

$$\Delta p_g = \epsilon \tag{B4}$$

the small number of (19).

In (B3) we have the (approximate) relation between the error in p_g and the corresponding error in p. For purposes of comparison, we are interested in the relative errors. We obtain approximations of the relative errors as follows:

$$\frac{\Delta p_g}{p_g} \sim \frac{f'(p)}{p_g}\ \Delta p = \frac{p}{p_g}\ f'(p) \left(\frac{\Delta p}{p}\right) \tag{B5}$$

which, upon rewriting, becomes

$$\left(\frac{\Delta p}{p}\right) \sim \frac{p_g}{p}\ \frac{1}{f'(p)} \left(\frac{\Delta p_g}{p_g}\right) \tag{B6}$$

To illustrate the use of (B6) let us consider the following seven measure functions whose relative errors are as tabulated.

Measure Function (p_g)	Relative Error Ratio $\left[\left(\frac{\Delta p}{p}\right)\Big/\left(\frac{\Delta p_g}{p_g}\right)\right]$	Location of Asymptote (p)
p	1	none
$2pq$	$\frac{1-p}{1-2p}$	0.50
$6p^2q^2$	$\frac{1-p}{2(1-2p)}$	0.50
$3p^2q$	$\frac{1-p}{2-3p}$	0.66
$4p^3q$	$\frac{1-p}{3-4p}$	0.75
$5p^4q$	$\frac{1-p}{4-5p}$	0.80
$p^4 + 4p^3q$	$\frac{4-3p}{12(1-p)}$	1.00

To aid in comparing the above tabulated functions, Fig. B1 has been drawn and shows how the relative error ratio $(\Delta p/p)/(\Delta p_g/p_g)$ varies with p. Of particular interest are those functions for which $|\Delta p/p|/|\Delta p_g/p_g| \leq 1$, representing direct utility of the selected value of ϵ as an upper bound of error.

The above tabulated functions are a sample of the possible functions which could be assigned to p_g. Once a particular functional relation is chosen for use in making measurements, an error analysis should serve to indicate the maximum error likely to be encountered within specific ranges of numerical values of p. From Fig. B1 the location of the asymptote, if one exists for a specific function, is a useful indicator of the region of gross errors. Because of this, the location of the asymptote is tabulated above for each of the functions.

It can be concluded that an error analysis can indicate the utility of a specific function in making measurements of p. Furthermore, for certain ranges of values of p, functions can be chosen such that $|\Delta p/p| \leq 1$, and the upper bound determined on the basis of p_g remains an upper bound for errors in p.

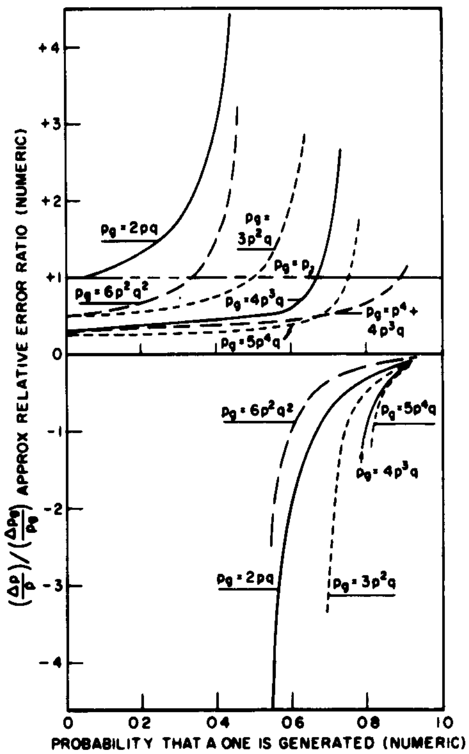


Fig. B1 - The dependence of the relative error ratio in measuring p upon p for seven measure groupings or number symbols

APPENDIX C

REPETITIVE SEQUENCES AND THEIR EFFECT ON GO/NO-GO TESTING OF RANDOMNESS

Suppose that a sequence of digits is obtained by repeating a group of fixed digits. If m_s is the number of binary digits which form the group of fixed digits, then a sequence of any length can be obtained merely by repeating the fixed group. The sequence thus obtained can be arranged in the form of an n by m array. The content obtained for the array will depend upon the way in which the sequence is sampled to derive entries for the array. Consider two ways of sampling (there are many ways which could be devised). In one sampling method, each digit of the sequence is used as it appears in the sequence and m-digit groups are formed from the sequence until there are n groups. In another method, the sequence is sampled to obtain m consecutive digits starting at arbitrary or essentially random places in the sequence, again until there are n groups.

To show how the array content can be derived, it is necessary to know what measure groups are to be used (i.e., p_g must be specified), as well as the count limits. With small values of m_s, and for small values of m, only a small number of entries need be made in the array because these entries are repeated. Once this repeated portion has been obtained it is easy enough to calculate the content of an array of any size.

The first sampling method has been used to investigate the following measure functions for the case where $p = 0.5$:

$M(45,55,100,p)$, $M(35,65,100,p)$, $(m = 1)$

$M(45,55,100,2pq)$, $M(35,65,100,2pq)$, $(m = 2)$

$M(32,43,100,3p^2q)$, $M(23,52,100,3p^2q)$, $(m = 3)$

$M(21,29,100,4p^3q)$, $M(12,38,100,4p^3q)$, $(m = 4)$

$M(12,19,100,5p^4q)$, $M(5,26,100,5p^4q)$, $(m = 5)$.

In each case the count limits, k_1 and k_2, were obtained from Fig. 5 at the appropriate values of p_g using first $x_k = \pm 1$ and then $x_k = \pm 3$. The results are given in Tables C1 through C4. Included in Tables C1 through C4 are the repeated portions of each sequence tried, i.e., the actual digital content of a repetition period. From the sequence of repeated groups of digits the array content is derived as described above; only that portion of the array which is repeated is shown. Repeated sequences are located together whenever, for a given value of m_s, the array contains the same m-digit groups, regardless of their order of occurrence. The sequences are tabulated, for each value of m, for increasing values of m_s. As a matter of interest the number of possible arrangements of digits for each value of m_s and m is given, i.e., the number of combinations of m_s things taken m at a time or of m things taken m_s at a time: $\binom{m_s}{m}$ when $m_s > m$, or $\binom{m}{m_s}$ when $m > m_s$. A given sequence is only considered once; for example, all zeros or all ones are considered once for each value of m. The group count is obtained by repeating the portion of the array which is shown an appropriate number of times, as determined from the value of n indicated for the particular measure function. It should be noted that when m_s is greater than m, the array content is readily obtained by taking the first m digits from each of the similar groups of repeated sequences given in the second column. Thus, for example, Table C4 might be used to investigate the effect of a value of $m_s = 7$ with the measure functions given in Table C3.

Table C1
Effect of Repeated Sequences $m = 1$ and 2

Repeated Sequence		Number of Digits Per Repetition Period (m_s)	Number of Possible Arrangements of Digits $\binom{m_s}{m}$	Portion of Array Which is Repeated for the Selected Groups	Measure Function Equation, Group Count, and Accept (A) or Reject (R) Indication for two Sequence Sampling Methods				
					Sequence Sampling Method I			Sequence Sampling Method II	
Number	Digits in One Repetition Period				Group Count From the Array (Numeric)	$x_k = \pm 1$	$x_k = \pm 3$	Group Count (Numeric) (Total variation of + 45 allowed)	$x_k = \pm 3$
$m = 1$, $p_g = p$: Selected Grouping 1; $p_g = 0.5$ at $p = 0.5$.						$M(45,55,100,p)$	$M(35,65,100,p)$		$M(455,545,1000,p)$
1	0...	1	1	0	0	R	R	0	R (all)
2	1...			1	100			1000	
3 4	01... 10...	2	4-2*	1 0	50	A	A	455 - 500	A (all)
$m = 2$, $p_g = 2pq$: Selected Groupings 01, 10; $p_g = 0.5$ at $p = 0.5$.						$M(45,55,100,2pq)$	$M(35,65,100,2pq)$	(Total var. ± 45 allowed)	$M(455,545,1000,2pq)$
1	0...	1	1	00	0	R	R	0	R (all)
2	1...			11					
3 4	01... 10...	2	4-2*	01 10	100			1000	
5 6 7	001... 010... 100...	3	8-2*	00 10 01	67			621 - 711	
8 9 10	110... 101... 011...			11 01 10					
11 12	0001... 0100...	4	16-4*	00 01	50	A	A	455 - 545	A (all)
13 14	0010... 1000...			00 10					
15 16	0011... 1100...			00 11	0	R	R	0	R (all)
17 18	0110... 1001...			01 10	100			1000	
19 20	1110... 1011...			11 10	50	A	A	455 - 545	A (all)
21 22	1101... 0111...			11 01					

*The second number indicates the number of arrangements previously considered.

Table C2
Effect of Repeated Sequences for $m = 3$

Repeated Sequence		Number of Digits Per Repetition Period (m_s)	Number of Possible Arrangements of Digits $\binom{m_s}{m}$	Portion of Array Which is Repeated for the Selected Groups	Measure Function Equation, Group Count, and Accept (A) or Reject (R) Indication				
					Sequence Sampling Method I			Sequence Sampling Method II	
Number	Digits in One Repetition Period				Group Count from the Array (Numeric)	$x_k = \pm 1$	$x_k = \pm 3$	Group Count (Numeric) (Total variation of ± 50 allowed)	$x_k = \pm 3$
$m = 3$, $p_g = 3p^2q$: Selected Groupings 110, 101, 011; $P_g = 0.375$ at $p = 0.5$						$M(23,52,100,3p^2q)$	$M(32,43,100,3p^2q)$		$M(325,425,1000,3p^2q)$
1	0...	1	1	000	0	R	R	0	R (all)
2	1...			111					
3 4	01... 10...	2	4 - 2*	010 101	50		A	450 - 550	
5 6 7	001... 010... 100...	3	8 - 2*	001 010 100	0		R	0	
8 9 10	110... 101... 011...			110 101 011	100			1000	
11 12 13 14	0001... 0010... 0100... 1000...	4	16 - 4*	000 100 010 001	0			0	
15 16 17 18	0011... 0110... 1100... 1001...			001 100 110 011	50		A	450 - 550	
19 20 21 22	1110... 1101... 1011... 0111...			111 011 101 110	75		R	700 - 800	
23 24 25 26 27	00001... 00010... 00100... 01000... 10000...	5	32 - 2*	000 010 000 100 001	0	R		0	
28 29 30 31 32	00011... 00110... 01100... 11000... 10001...			000 110 001 100 011	40	A	A	350 - 450	A (about 75% of range, or 0.93 probability) R (0.07 probability)
33 34 35 36 37	00101... 01001... 01010... 10010... 10100...			001 010 010 100 101	20	R	R	150 - 250	R (all)
38 39 40 41 42	11100... 01110... 11001... 10011... 00111...			111 001 110 011 100	40	A	A	350 - 450	A (0.93 probability) R (0.07 probability)
43 44 45 46 47	11010... 10110... 10101... 01101... 01011...			110 101 101 011 010	80	R	R	750 - 850	R (all)
48 49 50 51 52	01111... 10111... 11011... 11101... 11110...			011 110 111 101 111	60			550 - 650	

*The second number indicates the number of arrangements previously considered.

Table C3
Effect of Repeated Sequences for $m = 4$

Repeated Sequence		Number of Digits Per Repetition Period (m_s)	Number of Possible Arrangements of Digits $\binom{m_s}{m}$	Portion of Array Which is Repeated for the Selected Groups	Measure Function Equation, Group Count, and Accept (A) or Reject (B) Indication				
Number	Digits in One Repetition Period				Sequence Sampling Method I			Sequence Sampling Method II	
					Group Count From the Array (Numeric)	$x_k = \pm 1$	$x_k = \pm 3$	Group Count (Numeric) (Total variation of ± 45 allowed)	$x_k = \pm 3$
$m = 4$, $p_g = 4p^3q$: Selected Groupings 1110, 1101, 1011, 0111; $p_g = 0.25$ at $p = 0.5$						$M(21,29,100,4p^3q)$	$M(12,38,100,4p^3q)$		$M(208,292,1000,4p^3q)$
1	0...	1	1	0000	0	R	R	0	R (all)
2	1...			1111					
3	01...	2	4 - 2*	0101					
4	10...			1010					
5	001...	3	8 - 2*	0010					
6	010...			0100					
7	100...			1001					
8	110...			1101	67			621 - 711	
9	101...			1011					
10	011...			0110					
11	0001...	4	16 - 4*	1000	0			0	
12	0010...			0100					
13	0100...			0010					
14	1000...			0001					
15	0011...			0011					
16	0110...			0110					
17	1100...			1100					
18	1001...			1001					
19	1110...			1110	100			1000	
20	1101...			1101					
21	1011...			1011					
22	0111...			0111					
23	00001...	5	32 - 2*	0000	0			0	
24	00010...			1000					
25	00100...			0100					
26	01000...			0010					
27	10000...			0001					
28	00011...			0001					
29	00110...			1000					
30	01100...			1100					
31	11000...			0110					
32	10001...			0011					
33	00101...			0010					
34	01001...			1001					
35	01010...			0100					
36	10010...			1010					
37	10100...			0101					
38	11100...			1110	40			355 - 445	
39	01110...			0111					
40	11001...			0011					
41	10011...			1001					
42	00111...			1100					
43	11010...			1101					
44	10110...			0110					
45	10101...			1011					
46	01101...			0101					
47	01011...			1010					
48	01111...			0111	80			755 - 845	
49	10111...			1011					
50	11011...			1101					
51	11101...								

44 45 46 47	10110... 10101... 01101... 01011...			0110 1011 0101 1010					
48 49 50 51 52	01111... 10111... 11011... 11101... 11110...			0111 1011 1101 1110 1111	80			755 - 845	
53 54 55 56 57 58	000001... 000010... 000100... 001000... 010000... 100000...	6	64 - 10*	0000 0100 0001 0000 0010 1000	0			0	
59 60 61	000011... 001100... 110000...			0000 1100 0011					
62 63 64	000101... 010001... 010100...			0001 0100 0101					
65 66 67	100001... 000110... 011000...			1000 0110 0001					
68 69 70	001010... 100010... 101000...			0010 1000 1010					
71 72 73	000111... 011100... 110001...			0001 1100 0111	33		A	288 - 378	A (about 5% of range given by allowable limits) (or probability of accept = 0.003) R (probability of reject = 0.997)
74 75 76	001110... 100011... 111000...			0011 1000 1110					
77 78 79	001011... 101100... 110010...			0010 1100 1011					
80 81 82	001101... 010011... 110100...			0011 0100 1101					
83 84 85	010110... 011001... 100101...			0101 1001 0110	0		R	0	R (all)
86 87 88	011010... 100110... 101001...			0110 1001 1010					
89 90 91	001111... 110011... 111100...			0011 1100 1111					
92 93 94	010111... 011101... 110101...			0101 1101 0111	67	R		621 - 711	
95 96 97	011110... 100111... 111001...			0111 1001 1110					
98 99 100	101011... 101110... 111010...			1010 1110 1011					
101 102 103	011111... 110111... 111101...			0111 1101 1111					
104 105 106	101111... 111011... 111110...			1011 1110 1111					

*The second number indicates the number of arrangements previously considered.

Table C4
Effect of Repeated Sequences for $m = 5$

Repeated Sequence					Measure Function Equation and Accept (A) or Reject (R) Indication				
					Sequence Sampling Method I			Sequence Sampling Method II	
Number	Digits in One Repetition Period	Number of Digits Per Repetition Period (m_s)	Number of Possible Arrangements of Digits $\binom{m_s}{m}$	Portion of Array Which is Repeated for the Selected Groups	Group Count from the Array (Numeric)	$x_k = \pm 1$	$x_k = \pm 3$	Group Count (Numeric) (Total variation of ± 35 allowed)	$x_k = \pm 3$
$m = 5$, $p_g = 5p^4q$: Selected Groupings 11110, 11101, 11011, 10111, 01111; $p_g = 0.156$ at $p = 0.5$						$M(12,19,100,5p^4q)$	$M(5,26,100,5p^4q)$		$M(120,190,1000,5p^4q)$
1	0...	1	1	00000	0	R	R	0	R (all)
2	1...			11111					
3	01...	2	4 - 2*	01010					
4	10...			10101					
5	001...	3	8 - 2*	00100					
6	010...			10010					
7	100...			01001					
8	110...			11011	33			298 - 368	
9	101...			01101					
10	011...			10110					
11	0001...	4	16 - 4*	00010	0			0	
12	0010...			00100					
13	0100...			01000					
14	1000...			10001					
15	0011...			00110					
16	0110...			01100					
17	1100...			11001					
18	1001...			10011					
19	1110...			11101	75			715 - 785	
20	1101...			11011					
21	1011...			10111					
22	0111...			01110					
23	00001...	5	32 - 2*	00001	0			0	
24	00010...			00010					
25	00100...			00100					
26	01000...			01000					
27	10000...			10000					
28	00011...			00011					
29	00110...			00110					
30	01100...			01100					
31	11000...			11000					
32	10001...			10001					
33	00101...			00101					
34	01001...			01001					
35	01010...			01010					
36	10010...			10010					
37	10100...			10100					
38	11100...			11100					
39	01110...			01110					
40	11001...			11001					
41	10011...			10011					
42	00111...			00111					
43	11010...			11010					
44	10110...			10110					
45	10101...			10101					
46	01101...			01101					
47	01011...			01011					
48	01111...			01111	100			1000	
49	10111...			10111					
50	11011...			11011					
51	11101...			11101					

28	00011...			00011					
29	00110...			00110					
30	01100...			01100					
31	11000...			11000					
32	10001...			10001					
33	00101...			00101					
34	01001...			01001					
35	01010...			01010					
36	10010...			10010					
37	10100...			10100					
38	11100...			11100					
39	01110...			01110					
40	11001...			11001					
41	10011...			10011					
42	00111...			00111					
43	11010...			11010					
44	10110...			10110					
45	10101...			10101					
46	01101...			01101					
47	01011...			01011					
48	01111...			01111	100			1000	
49	10111...			10111					
50	11011...			11011					
51	11101...			11101					
52	11110...			11110					
53	000001...	6	64 - 10*	00000	0			0	
54	000010...			10000					
55	000100...			01000					
56	001000...			00100					
57	010000...			00010					
58	100000...			00001					
59	000011...			00001					
60	001100...			10000					
61	110000...			11000					
65	100001...			01100					
66	000110...			00110					
67	011000...			00011					
62	000101...			00010					
63	010001...			10001					
64	010100...			01000					
68	001010...			10100					
69	100010...			01010					
70	101000...			00101					
71	000111...			00011					
72	011100...			10001					
73	110001...			11000					
74	001110...			11100					
75	100011...			01110					
76	111000...			00111					
77	001011...			00101					
78	101100...			10010					
79	110010...			11001					
83	010110...			01100					
84	011001...			10110					
85	100101...			01011					
80	001101...			00110					
81	010011...			10011					
82	110100...			01001					
86	011010...			10100					
87	100110...			11010					
88	101001...			01101					
89	001111...			00111	33			298-368	
90	100111...			10011					
91	011110...			11001					
92	110011...			11100					
93	111001...			11110					
94	111100...			01111		R	R		R (all)

2

*The second number indicates the number of arrangements previously considered.

Table C4 (Continued)
Effect of Repeated Sequences for $n = 5$

Repeated Sequence		Number of Digits Per Repetition Period (n_s)	Number of Possible Arrangements of Digits $\binom{n_s}{n}$	Portion of Array Which is Repeated for the Selected Groups	Measure Function Equation and Accept (A) or Reject (R) Indication				
Number	Digits in One Repetition Period				Sequence Sampling Method I			Sequence Sampling Method II	
					Group Count from the Array (Numeric)	$x_k = \pm 1$	$x_k = \pm 3$	Group Count (Numeric) (Total variation of ± 35 allowed)	$x_k = \pm 3$
$n = 5$, $P_g = 5p^4q$: Selected Groupings 11110,11101,11011, 10111,01111; $P_g = 0.156$ at $p = 0.5$						$M(12,19,100,5p^4q)$	$M(5,26,100,5p^4q)$		$M(120,190,1000,5p^4q)$
95 96 97 98 99 100	010111... 011101... 101011... 101110... 110101... 111010...	6	64 - 10*	01011 10101 11010 11101 01110 10111	33	R	R	298 - 368	R (all)
101 102 103 104 105 106	011111... 101111... 110111... 111011... 111101... 111110...			01111 10111 11011 11101 11110 11111	83			798 - 868	
107 108 109 110 111 112 113	0000001... 0000010... 0000100... 0001000... 0010000... 0100000... 1000000...	7	128 - 2*	00000 01000 00010 00000 10000 00100 00001	0			0	
114 115 116 117 118 119 120	0000011... 0000110... 0001100... 0011000... 0110000... 1100000... 1000001...			00000 11000 00110 00001 10000 01100 00011					
121 122 123 124 125 126 127	0000101... 0001010... 0010100... 0101000... 1010000... 1000010... 0100001...			00001 01000 01010 10000 10100 00010 00101					
128 129 130 131 132 133 134	0001001... 0010001... 0010010... 0100010... 0100100... 1000100... 1001000...			00010 01000 10010 00100 10001 00100 01001					
135 136 137 138 139 140 141	0000111... 0001110... 0011100... 0111000... 1000011... 1100001... 1110000...			00001 11000 01110 00011 10000 11100 00111					
142 143 144 145	0001011... 0010110... 0101100... 0110001...			00010 11000 10110 00101					

119	1100000...	2		01100					
120	1000001...			00011					
121	0000101...			00001					
122	0001010...			01000					
123	0010100...			01010					
124	0101000...			10000					
125	1010000...			10100					
126	1000010...			00010					
127	0100001...			00101					
128	0001001...			00010					
129	0010001...			01000					
130	0010010...			10010					
131	0100010...			00100					
132	0100100...			10001					
133	1000100...			00100					
134	1001000...			01001					
135	0000111...			00001					
136	0001110...			11000					
137	0011100...			01110					
138	0111000...			00011					
139	1000011...			10000					
140	1100001...			11100					
141	1110000...			00111					
142	0001011...			00010					
143	0010110...			11000					
144	0101100...			10110					
145	0110001...			00101					
146	1000101...			10001					
147	1011000...			01100					
148	1100010...			01011					
149	0001101...			00011					
150	0011010...			01000					
151	0100011...			11010					
152	0110100...			00110					
153	1000110...			10100					
154	1010001...			10100					
155	1101000...			01101					
156	0010011...			00100					
157	0011001...			11001					
158	0100110...			00110					
159	0110010...			01001					
160	1001001...			10010					
161	1001100...			01100					
163	1100100...			10011					
164	0010101...			00101					
165	0100101...			01001					
166	0101001...			01010					
167	0101010...			01010					
168	1001010...			10010					
169	1010010...			10100					
170	1010100...			10101					
171	0001111...			00011	29	R	R	251 - 321	R (all)
172	0011110...			11000					
173	0111100...			11110					
174	1000111...			00111					
175	1100011...			10001					
176	1110001...			11100					
177	1111000...			01111					
178	0010111...			00101	14	A	A	108 - 178	A (approx. 83% of range of limits overlap; 0.97% accept probability) R (0.03 reject probability)
179	0101110...			11001					
180	0111001...			01110					
181	1011100...			01011					
182	1100101...			10010					
183	1110010...			11100					
184	1001011...			10111					

*The second number indicates the number of arrangements previously considered.

The results obtained using method I and shown in Tables C1 through C4 are summarized in Table C5. The purpose in choosing two measure functions for each value of m was to demonstrate that different count limits (k_1 and k_2) can have somewhat different repeated sequence effects. While the difference can be clearly seen from Table C5 (e.g., the measure functions for $m = 3$ and 4), such a drastic change in limits would not be recommended without ascertaining the change in acceptance characteristic and the associated change in the incidence of reject indications. This trivial example serves to illustrate how far it may be necessary to alter the limits in some cases to achieve a significant change in accept indication in the presence of repeated sequences.

Table C5
Repeated Sequences Which Cause Accept Indications for the Measure Functions Being Tested

Sequence Sampling Method	Measure Function	m	m_s	Repeated Sequence Numbers Which Give Accept Indications (from Tables C1 through C4)	Approximate Probability of Accept Indication (Numeric)
I	$M(45,55,100,p)$	1	2	3,4	1
	$M(35,65,100,p)$				
II	$M(455,545,1000,p)$				
I	$M(45,55,100,2pq)$	2	4	11 through 14 19 through 22	
	$M(35,65,100,2pq)$				
II	$M(455,545,1000,2pq)$				
I	$M(32,43,100,3p^2q)$	3	5	28 through 32	
	$M(23,52,100,3p^2q)$		2	3,4	
			4	15 through 18	
			5	28 through 32 38 through 42	
II	$M(325,425,1000,3p^2q)$				0.93
I	$M(21,29,100,4p^3q)$	4	7	135 through 141 171 through 177	1
	$M(12,38,100,4p^3q)$		6	71 through 82	
			7	135 through 141 149 through 155 171 through 177	
II	$M(208,292,1000,4p^3q)$		6	71 through 82	0.003
			7	135 through 141 171 through 177	0.74
I	$M(12,19,100,5p^4q)$	5	7	178 through 184	1
	$M(5,26,100,5p^4q)$				
II	$M(120,190,1000,5p^4q)$				0.97

Next let us consider method II. Now we are concerned with a sequence which is made up, as before, with a group of fixed digits m_s, which are repeated. In sampling a sequence, arbitrary or (assumed) random places are taken to select an entry of m digits for making up the array. To illustrate the process we will consider the following measure functions:

$$M(455,545,1000,p) \qquad M(455,545,1000,2pq) \qquad M(325,425,1000,3p^2q)$$

$$M(208,292,1000,4p^3q) \qquad M(120,190,1000,5p^4q).$$

For each sequence to be tried, the array content is determined as in the case of the first sampling method; hence, the entries of Tables C1 through C4, which include the portions of the arrays which are repeated, are applicable in this sampling method. In this case it is necessary to assign (in practice, to determine) the variation in count which is likely to occur; for our example, a random selection of entries in the repeated portion of the array has been assumed. It is natural to assume that in the long run a normal distribution of entries should be obtained. It will be noted that the limits for each of the measure functions have been obtained from Fig. 6, at the appropriate value of p_g (corresponding to $p = 0.5$), for $x_k = \pm 3$. This assignment of limits permits a nearly normal variation in count to be obtained under normal circumstances; the range of this distribution is 6σ. For purposes of illustration, the expected count is assumed to have the same type of distribution – a normal distribution with about the same value of σ. Therefore the value of total variation is taken to be $\pm 3\sigma$, where

$$\sigma = \frac{k_2 - k_1}{6} \tag{C1}$$

and k_1 and k_2 are, respectively, the lower and upper limits of count taken from the measure function.

In Tables C1 through C4 each of the above measure functions is investigated. For each function the total variation ($\pm 3\sigma$) is given, using the value of σ obtained from (C1). Where appropriate, the total variation is included in the group count. The expected group count is compared with the measure function limits (k_1, k_2) and the expected indication is noted (R = reject, or A = accept). In method II, when the group count is compared with the measure function limits, it is found in some cases that only part of the expected count falls within the accept limits. In these cases it is necessary to determine the approximate probability of getting an accept indication. The example we have chosen, which does not give tolerances on p, is assumed to have an acceptance characteristic which is the normal curve. With this assumption, the probability of acceptance can be readily determined; this calculated value is given in the tables.

For purposes of comparison, Table C5 includes the accept indications obtained for both sequence sampling methods. The results shown by Table C5 are indicative of what can be expected from an investigation into the effect of repeated sequences on a go/no-go test device. The measure functions with the wider, more realistically set limits are more vulnerable to sampling by method I.

The foregoing discussion serves to point out the nature of the problem which arises with repeated sequences. The examples used are not realistic, but they have served to illustrate some of the conclusions which can be drawn. It is appropriate to consider the measure functions used in the latter part of the report, as possibly, a more realistic demonstration.

The three measure functions being considered now are the following:

$$M(438,538,1000,p)$$

$$M(310,410,1000,6p^2q^2)$$

and

$$M(225,372,1000,p^4+4p^3q).$$

For each of these measure functions, the acceptance curve is available, Figs. 13, 14, and 15, respectively. We will consider each of these functions and show the reaction to repeated sequences when sampled by both methods I and II.

Let us consider the formation of arrays in which $m = 4$ for each of these functions. This poses a problem insofar as the first of the three functions is concerned; for purposes of illustration it is considered that a single column sum (one of the four obtainable from the 4-digit array) will be used. It is interesting to note that a simplification in tabulation is achieved if the hexadecimal number system is used to write the array entries. The conversions for the sequences of Table C4 are given in Table C6. Table C7 includes the hexadecimal numbers used. In Table C8 are shown the binary and hexadecimal digits of some specific groupings.

Having set up the procedure for obtaining arrays, use can be made of the sequences listed in Table C4, the most extensive of the tables, to test the measure functions just listed. Using both methods of sequence sampling, the effect of each of the sequences can be obtained; however, it is first necessary to allow a variation in count for method II, as was done previously. For our purposes, a count variation of ± 50 is considered suitable, since this value is very nearly obtained from Fig. 5 ($n = 1000$) for any of the limits used. The results are given in Table C9; a summary of these results is given in Table C10.

From the summary, Table C10, we find that out of the 184 sequences for sampling method I there are 24 accept indications obtained from use of the first two measure functions, and only 13 with the third. In the case of sampling by method II, the first two measure functions give 83 and 59 accept indications respectively; the third, only 23. Of the first two measure functions, the second gives values of the probability of acceptance which are lower, for sampling by method II.

It should be noted that the conclusion previously obtained regarding the better ability of Method I to make tests is not substantiated in Table C10. The inability to verify a conclusion merely points up the inability to specify a general or absolute method of testing for the effect of repeated sequences.

Table C6
Array (m = 4) Content of Repeated Sequences Expressed in Hexadecimal Notation

Sequence Number (from Table C4)	Array Content Hexadecimal Notation (see Table C7)	Number of Digits per period (m_g)
1	0	1
2	f	
3,4	5,a	2
5,6,7	2,4,9	3
8,9,10	6,b,d	
11-14	1,2,4,8	4
15-18	3,6,9,c	
19-22	7,b,d,e	
23-27	0,1,2,4,8	5
28-32	1,3,6,8,c	
33-37	2,4,5,9,a	
38-42	3,7,9,c,e	
43-47	5,6,a,b,d	
48-52	7,b,d,e,f	
53-58	0,1,2,4,8	6
59-61,65-67	0,1,3,6,8,c	
62-64,68-70	1,2,4,5,8,a	
71-76	1,3,7,8,c,e	
77-79,83-85	2,5,6,9,b,c	
80-82,86-88	2,3,6,9,a,d	
89-94	3,7,9,c,e,f	
95-100	5,7,a,b,d,e	
101-106	7,b,d,e,f	
107-113	0,1,2,4,8	7
114-120	0,1,3,6,8,c	
121-127	0,1,2,4,5,8,a	
128-134	1,2,4,8,9	
135-141	0,1,3,7,8,c,e	
142-148	1,2,5,6,8,b,c	
149-155	1,3,4,6,a,d	
156-163	2,3,4,6,9,c	
164-170	2,4,5,9,a	
171-177	1,3,7,8,c,e,f	
178-184	2,5,7,9,b,c,e	

Table C7
Hexadecimal Number Equivalents

Notation	
Binary	Hexadecimal
0000	0
0001	1
0010	2
0011	3
0100	4
0101	5
0110	6
0111	7
1000	8
1001	9
1010	a
1011	b
1100	c
1101	d
1110	e
1111	f

Table C8
Digital Groups Associated with Some Specific Grouping Functions

Binary	Hexadecimal	Measure Group (equation for p_g)	
0000	0	q^4	
0001 0010 0100 1000	1 2 4 8	$4pq^3$	
0011 0101 0110 1001 1010 1100	3 5 6 9 a c	$6p^2q^2$	
0111 1011 1101 1110	7 b d e	$4p^3q$	$p^4 + 4p^3q$
1111	f	p^4	

Table C9
Effect of Repeated Sequences on Three Measure Functions

Repeated Sequence* (Number)	M(438,538,1000,p)					M(310,410,1000,$6p^2q^2$)					M(225,372,1000,p^4+4p^3q)				
	Sampling Method I		Sampling Method II		Prob. of Acceptance	Sampling Method I		Sampling Method II		Prob. of Acceptance	Sampling Method I		Sampling Method II		Prob. of Acceptance
	Expected Count	A (Accept) R (Reject)	Expected Count	A (Accept) R (Reject)		Expected Count	A (Accept) R (Reject)	Expected Count	A (Accept) R (Reject)		Expected Count	A (Accept) R (Reject)	Expected Count	A (Accept) R (Reject)	
1	0	R	0	R	0	0	R	0	R	0	0	R	0	R	0
2	1000		1000								1000		1000		
3,4	500	A	450-550	A,R	0.99,0.01	1000		1000			0		0		
5,6,7	333	R	283-383	R	0	333	A	283-383	A,R	0.91,0.09					
8,9,10	666		616-716								666		616-716		
11-14	250		200-300			0	R	0	R	0	0		0		
15-18	500	A	450-550	A,R	0.99,0.01	1000		1000							
19-22	750	R	700-800	R	0	0		0			1000		1000		
23-27	200		150-250								0		0		
28-37	400		350-450	A,R	0.01,0.99	600		550-650							
38-47	600		550-650	R	0						400		350-450	A,R	0.05,0.95
48-52	800		750-850			0		0			1000		1000	R	0
53-58	166		116-216								0		0		
59-61,65-67	333		283-383			500		550-650							
62-64,68-70						333	A	283-383	A,R	0.91,0.09					
71-76	500	A	450-550	A,R	0.99,0.01						333	A	283-383	A,R	0.99,0.01
77-88						666	R	616-716	R	0	166	R	116-216	R	0
89-94	666	R	616-716	R	0	500		550-650			500		450-550		
95-100						333	A	283-383	A,R	0.91,0.09	666		616-716		
101-106	833		783-883			0	R	0	R	0	1000		1000		
107-113	143		93-193								0		0		
114-120	287		237-337			429		379-479	A,R	0.13,0.87					
121-127						287		237-337		0.06,0.92					
128-134						143		93-193	R	0					
135-141	429		379-479	A,R	0.29,0.71	287		237-337	A,R	0.06,0.92	287	A	237-337	A	1
142-148						429		379-479		0.13,0.87	143	R	93-193	R	0
149-155						571		521-621	R	0					
	571		521-621		0.02,0.98										
156-170	429		379-479		0.29,0.71	714		664-764			0		0		
171-177	571		521-621		0.02,0.98	287		237-337	A,R	0.06,0.92	429		379-479		
178-184						429		379-479		0.13,0.87					

*From Table C4.

Table C10
Summary of Repeated Sequences Which Cause Acceptance Indications by Three Measure Functions

Repeated Sequence Identification Numbers	Number of Repeated Sequences	Digit-Group Content of Array (Hexadec. Notation)	Number of Digits Per Period (n_s)	$M(438,538,1000,p)$		$M(310,410,1000,6p^2q^2)$		$M(225,372,1000,p^4+4p^3q)$	
				Sampling Method	Prob. of Accept. (Numeric)	Sampling Method	Prob. of Accept. (Numeric)	Sampling Method	Prob. of Accept. (Numeric)
3,4	2	5,a	2	I,II	1,0.99				
5,6,7	3	2,4,9	3			I,II	1,0.91		
8,9,10		6,b,d							
15-18	4	3,6,9,c	4	I,II	1,0.99				
28-32	5	1,3,6,8,c	5	II	0.01				
33-37		2,4,5,9,a			0.01				
38-42		3,7,9,c,e							
43-47		5,6,a,b,d						II	0.05
62,63,64,68,69,70		1,2,4,5,8,a				I,II	1,0.91		
71-76		1,3,7,8,c,e			1,0.99		1,0.91	I,II	1,0.99
77,78,79,83,84,85	6	2,5,6,9,b,c	6	I,II	1,0.99				
80,81,82,86,87,88		2,3,6,9,a,d			1,0.99				
95-100		5,7,a,b,d,e					1,0.91		
114-120		0,1,3,6,8,c				II	0.13		
121-127		0,1,2,4,5,8,a					0.08		
135-141		0,1,3,7,8,c,e			0.29			I,II	1
142-148		1,2,5,6,8,b,c			0.29	II	0.13		
149-155	7	1,3,4,6,a,d	7		0.02 or 0.29				
156-163		2,3,4,6,9,c		II	0.29				
164-170		2,4,5,9,a			0.29				
171-177		1,3,7,8,c,e,f			0.02	II	0.08		
178-184		2,5,7,9,b,c,e			0.002		0.13		

UNCLASSIFIED

Naval Research Laboratory. Report 5730.
SOME ASPECTS OF GO/NO-GO TESTING OF RANDOMNESS OF CONTINUALLY GENERATED BINARY DIGITS, by H. M. Suski. 52 pp. and figs., March 1, 1962.

Pseudorandom numbers can be obtained statically, i.e., from a table of random numbers, or they may be generated continually (dynamically). Static cases have been investigated; e.g., tables of random digits often contain results of tests. The dynamic case, however, implies that tests for randomness be made continually. Go/no-go methods are attractive.

Problems associated with measuring randomness in the dynamic case of a generator continually producing binary digits are investigated. The mathematics of Bernoulli trials serves as the model against which the performance of the generator is compared. It is shown that there are a large number of ways in which a measuring system might be attempted. Such systems are based on explicit functions (called measure functions) of p, the probability that a "one" is generated.

Since the digits can be grouped (a group consists of m-digits), a binomial expansion $[p + (1 - p)]^m$ can be written for each value of m. Any term or combination of terms of any expansion can serve as a measure group, the basis of a measure function.

A typical measuring problem involves the case where p is constant and has a value within specified tolerances. A go/no-go measurement indicates that p is within the specified tolerances.

UNCLASSIFIED (over)

1. Random distribution - Test methods
I. Suski, H. M.

UNCLASSIFIED

Naval Research Laboratory. Report 5730.
SOME ASPECTS OF GO/NO-GO TESTING OF RANDOMNESS OF CONTINUALLY GENERATED BINARY DIGITS, by H. M. Suski. 52 pp. and figs., March 1, 1962.

Pseudorandom numbers can be obtained statically, i.e., from a table of random numbers, or they may be generated continually (dynamically). Static cases have been investigated; e.g., tables of random digits often contain results of tests. The dynamic case, however, implies that tests for randomness be made continually. Go/no-go methods are attractive.

Problems associated with measuring randomness in the dynamic case of a generator continually producing binary digits are investigated. The mathematics of Bernoulli trials serves as the model against which the performance of the generator is compared. It is shown that there are a large number of ways in which a measuring system might be attempted. Such systems are based on explicit functions (called measure functions) of p, the probability that a "one" is generated.

Since the digits can be grouped (a group consists of m-digits), a binomial expansion $[p + (1 - p)]^m$ can be written for each value of m. Any term or combination of terms of any expansion can serve as a measure group, the basis of a measure function.

A typical measuring problem involves the case where p is constant and has a value within specified tolerances. A go/no-go measurement indicates that p is within the specified tolerances.

UNCLASSIFIED (over)

1. Random distribution - Test methods
I. Suski, H. M.

UNCLASSIFIED

Naval Research Laboratory. Report 5730.
SOME ASPECTS OF GO/NO-GO TESTING OF RANDOMNESS OF CONTINUALLY GENERATED BINARY DIGITS, by H. M. Suski. 52 pp. and figs., March 1, 1962.

Pseudorandom numbers can be obtained statically, i.e., from a table of random numbers, or they may be generated continually (dynamically). Static cases have been investigated; e.g., tables of random digits often contain results of tests. The dynamic case, however, implies that tests for randomness be made continually. Go/no-go methods are attractive.

Problems associated with measuring randomness in the dynamic case of a generator continually producing binary digits are investigated. The mathematics of Bernoulli trials serves as the model against which the performance of the generator is compared. It is shown that there are a large number of ways in which a measuring system might be attempted. Such systems are based on explicit functions (called measure functions) of p, the probability that a "one" is generated.

Since the digits can be grouped (a group consists of m-digits), a binomial expansion $[p + (1 - p)]^m$ can be written for each value of m. Any term or combination of terms of any expansion can serve as a measure group, the basis of a measure function.

A typical measuring problem involves the case where p is constant and has a value within specified tolerances. A go/no-go measurement indicates that p is within the specified tolerances.

UNCLASSIFIED (over)

1. Random distribution - Test methods
I. Suski, H. M.

UNCLASSIFIED

Naval Research Laboratory. Report 5730.
SOME ASPECTS OF GO/NO-GO TESTING OF RANDOMNESS OF CONTINUALLY GENERATED BINARY DIGITS, by H. M. Suski. 52 pp. and figs., March 1, 1962.

Pseudorandom numbers can be obtained statically, i.e., from a table of random numbers, or they may be generated continually (dynamically). Static cases have been investigated; e.g., tables of random digits often contain results of tests. The dynamic case, however, implies that tests for randomness be made continually. Go/no-go methods are attractive.

Problems associated with measuring randomness in the dynamic case of a generator continually producing binary digits are investigated. The mathematics of Bernoulli trials serves as the model against which the performance of the generator is compared. It is shown that there are a large number of ways in which a measuring system might be attempted. Such systems are based on explicit functions (called measure functions) of p, the probability that a "one" is generated.

Since the digits can be grouped (a group consists of m-digits), a binomial expansion $[p + (1 - p)]^m$ can be written for each value of m. Any term or combination of terms of any expansion can serve as a measure group, the basis of a measure function.

A typical measuring problem involves the case where p is constant and has a value within specified tolerances. A go/no-go measurement indicates that p is within the specified tolerances.

UNCLASSIFIED (over)

1. Random distribution - Test methods
I. Suski, H. M.

UNCLASSIFIED

Means are provided for the setting of measure group-count tolerances; a count alone then provides the indication of an acceptable or nonacceptable value of p. The sample size is selected on the basis of the desired confidence limit or the upper bound of the error in measuring p.

Since there are many possible measure functions, some means is required for comparing the relative effectiveness of different functions. A useful method of comparison is available if measure function "acceptance" characteristics are plotted. An acceptance characteristic is a plot of the probability that the measure group digits occur within the determined group-count tolerances. The acceptance characteristic is plotted for the results obtained from a single application of a particular measure function. By requiring a sequence of applications of the same measure function and by introducing an acceptance decision criterion, the acceptance characteristic more nearly approaches the ideal.

Under certain conditions, a failure of the generator might manifest itself by the appearance of a repeated sequence of digits. Some of the necessary conditions are investigated for a go/no-go measuring system to breakdown, i.e., to give erroneous "accept" or "go" readings for an input consisting of specific repeated sequences. It is found that immunity from breakdown is dependent upon the number of digits in the group used in the measure function; the longer the group, the longer is the sequence of digits which can cause an erroneous indication—thus, more immunity.

The various aspects of the problem of a dynamic measurement of randomness are illustrated in an arbitrary example. Results are obtained for three measure functions.

In developing the theory, a method for measuring p was obtained; it provides an independent method useful in checking the go/no-go results.

UNCLASSIFIED

UNCLASSIFIED

Means are provided for the setting of measure group-count tolerances; a count alone then provides the indication of an acceptable or nonacceptable value of p. The sample size is selected on the basis of the desired confidence limit or the upper bound of the error in measuring p.

Since there are many possible measure functions, some means is required for comparing the relative effectiveness of different functions. A useful method of comparison is available if measure function "acceptance" characteristics are plotted. An acceptance characteristic is a plot of the probability that the measure group digits occur within the determined group-count tolerances. The acceptance characteristic is plotted for the results obtained from a single application of a particular measure function. By requiring a sequence of applications of the same measure function and by introducing an acceptance decision criterion, the acceptance characteristic more nearly approaches the ideal.

Under certain conditions, a failure of the generator might manifest itself by the appearance of a repeated sequence of digits. Some of the necessary conditions are investigated for a go/no-go measuring system to breakdown, i.e., to give erroneous "accept" or "go" readings for an input consisting of specific repeated sequences. It is found that immunity from breakdown is dependent upon the number of digits in the group used in the measure function; the longer the group, the longer is the sequence of digits which can cause an erroneous indication—thus, more immunity.

The various aspects of the problem of a dynamic measurement of randomness are illustrated in an arbitrary example. Results are obtained for three measure functions.

In developing the theory, a method for measuring p was obtained; it provides an independent method useful in checking the go/no-go results.

UNCLASSIFIED

UNCLASSIFIED

Means are provided for the setting of measure group-count tolerances; a count alone then provides the indication of an acceptable or nonacceptable value of p. The sample size is selected on the basis of the desired confidence limit or the upper bound of the error in measuring p.

Since there are many possible measure functions, some means is required for comparing the relative effectiveness of different functions. A useful method of comparison is available if measure function "acceptance" characteristics are plotted. An acceptance characteristic is a plot of the probability that the measure group digits occur within the determined group-count tolerances. The acceptance characteristic is plotted for the results obtained from a single application of a particular measure function. By requiring a sequence of applications of the same measure function and by introducing an acceptance decision criterion, the acceptance characteristic more nearly approaches the ideal.

Under certain conditions, a failure of the generator might manifest itself by the appearance of a repeated sequence of digits. Some of the necessary conditions are investigated for a go/no-go measuring system to oreakdown, i.e., to give erroneous "accept" or "go" readings for an input consisting of <pecific repeated sequences. It is found that immunity from breakdown is dependent upon the number of digits in the group used in the measure function; the longer the group, the longer is the sequence of digits which can cause an erroneous indication—thus, more immunity.

The various aspects of the problem of a dynamic measurement of randomness are illustrated in an arbitrary example. Results are obtained for three measure functions.

In developing the theory, a method for measuring p was obtained; it provides an independent method useful in checking the go/no-go results.

UNCLASSIFIED

UNCLASSIFIED

Means are provided for the setting of measure group-count tolerances; a count alone then provides the indication of an acceptable or nonacceptable value of p. The sample size is selected on the basis of the desired confidence limit or the upper bound of the error in measuring p.

Since there are many possible measure functions, some means is required for comparing the relative effectiveness of different functions. A useful method of comparison is available if measure function "acceptance" characteristics are plotted. An acceptance characteristic is a plot of the probability that the measure group digits occur within the determined group-count tolerances. The acceptance characteristic is plotted for the results obtained from a single application of a particular measure function. By requiring a sequence of applications of the same measure function and by introducing an acceptance decision criterion, the acceptance characteristic more nearly approaches the ideal.

Under certain conditions, a failure of the generator might manifest itself by the appearance of a repeated sequence of digits. Some of the necessary conditions are investigated for a go/no-go measuring system to breakdown, i.e., to give erroneous "accept" or "go" readings for an input consisting of specific repeated sequences. It is found that immunity from breakdown is dependent upon the number of digits in the group used in the measure function; the longer the group, the longer is the sequence of digits which can cause an erroneous indication—thus, more immunity.

The various aspects of the problem of a dynamic measurement of randomness are illustrated in an arbitrary example. Results are obtained for three measure functions.

In developing the theory, a method for measuring p was obtained; it provides an independent method useful in checking the go/no-go results.

UNCLASSIFIED